

DPF-Series 产品技术与配置指南

Ver　　1.0

友讯电子设备（上海）有限公司

2007-07

www.dlink.com.cn

版本更新纪录

版本号	软件版本	作者	审核	**1．变更描述** **2．审核结果**	发布者 时间
1.0	**DPF :1.7.2.2**			create	2007-07-17

目录

1 前言

感谢您使用D-Link全能策略流控产品，本手册介绍了 DPF-Series 设备的基本功能、产品技术及配置原理，包括主要功能的典型案例，其主要章节介绍以下内容：

- WebUI 描述与约定
- 管理接口，包括 WEB 网管和 CLI 网管
- 物理接口，物理接口参数的介绍和相关参数的修改
- 虚拟接口，虚拟接口的原理介绍和配置方法
- 安全区域，安全区域的原理介绍及配置方法
- 系统升级，包括 FTP/TFTP 和 HTTP 升级
- 透明模式，透明模式的虚拟接口的原理介绍和典型案例
- 路由模式，路由模式的虚拟接口的原理介绍和典型案例
- 网络地址转换，原理介绍和典型案例，包括 NAT、PAT、服务映射
- 策略路由，原理介绍和典型案例
- 安全策略，原理介绍和典型案例，以及常见问题的疑难解答
- 用户认证，包括用户认证原理介绍和典型案例，还涉及用户日志、IP 统计、黑名单和 QoS 的使用方法和案例介绍
- DHCP，DHCP 服务器、DHCP 中继代理、DHCP 透明模式等三种 DHCP 角色的原理介绍和典型案例。
- LOG，包括各种日志的原理、查询方法
- 入侵检测，原理介绍和典型案例
- IM&P2P，介绍怎样控制各种 IM&P2P 软件，以及配置方法
- 服务控制，提供了多种方法来对上至 7 层的网络协议进行分类、分析和管理。

2 WEB描述与约定

贯穿本手册的全部篇章，用一个箭头符号(->) 来指示在 WebUI 中导航，其方法是单击菜单选项和链接。例如，新增一个 vif 的对话框的路径显示为：**网络配置(NETWORK)->网络接口(Interfaces)->Virtual ->新增(Create New)**

如要用 WebUI 执行任务，必须首先导航到相应的对话框，然后可在该对话框中定义对象和设置参数。每个任务的指令集划分为两部分: 导航路径和配置详细信息。例如，下列指令集包含添加一条默认路由的配置对话框的路径和要配置的设置：

进入 **网络配置(NETWORK)->路由配置(Routing)->网络路由(Static Routing)->新增(Create New)**，添加一条到 1.1.1.250 的默认路由

新增网络路由表 提交 取消 返回

IP地址	0.0.0.0	子网掩码	0.0.0.0
网关/ISP	1.1.1.250		

*IP地址 0.0.0.0 掩码 0.0.0.0 代表缺省路由

当前配置

序号	设置
共 1 条记录 当前第 1 页	
1	set nm-if wan1 ip 192.168.0.1 netmask 255.255.255.0

- 图标（ICON）约定：

图标	含义	图标	含义	图标	含义
	地址分配		修改密码		插入
	成员		清除		剪切
	删除		DSA key更改		进入
	防火墙		细节		主机列表
	密钥导入		锁定		解锁
	编辑		策略移动		协议
	统计信息		状态		目标

- 系统约定功能 的使用，从左向右依次作如下解释：

1．系统帮助。

2．系统保存功能，点击它会弹出保存设置对话框如图：

请选择保存设置条件 保存 关闭

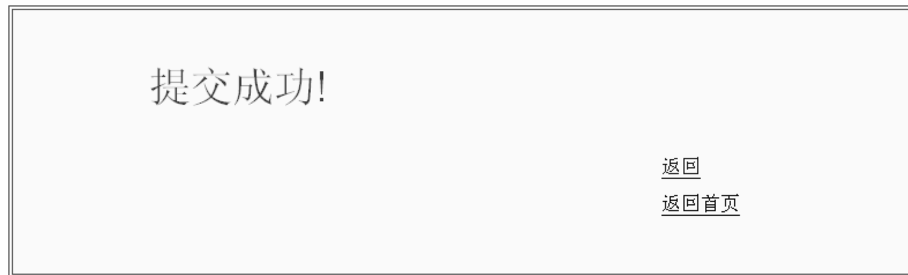
当前 LKG 配置

"当前"表示当前所在虚系统的配置， "LKG 成功配置"指的是上一次提交成功并保存的配置。

3．系统离开功能，点击它则系统退出 web 管理重新回到登陆界面。

4．系统重启功能，点击它弹出"重启前您要保存设置么？"点击"**确定**"打开调用保存功能，点击"**取消**"系统重新启动。

- 提交成功：
  在每次设置参数后，点击“**提交**”按钮，如果提交成功，显示如下提示：



点击“**返回**”**，**回到刚才的配置示页面，查看提交后的信息。点击“**返回首页**”**，**则系统回到首页。

- **“页首”**和**“页尾”**功能标志，当处于页首时，点击右上角的**“页尾”**则会跳到页尾，反之亦然。
  当页面带有新增功能时，如果页面内容显示超过屏幕显示范围，也会在页首添加**新增**功能按钮。

3 设备安装

DPF-Series 设备的安装分以下几个步骤：

1. 插上电源，启动设备。
2. 须用**交叉线**将 PC 的网卡与 DPF-Series 设备的 OIF1 接口相连。OIF1 口右上角的 Link 灯亮了，表示连接成功。
3. 配置 PC 的网卡 IP 地址。缺省情况下，OIF1 接口的 IP 地址为 192.168.0.1/24，所以将网卡的 IP 地址配置到 192.168.0.0/24 网段。
4. 启动 IE，在地址栏中输入 https://192.168.0.1:8080，则弹出登陆对话框，提示输入用户名和密码。缺省的登陆用户名为 root，密码为 root*PWD。如下图：
5. 正确输入用户名和密码之后，进入 web 网管的主界面。

4 系统升级

4.1 简介

DPF-Series 设备支持 FTP、TFTP 和 HTTP 三种升级方式。 FTP 和 TFTP 升级需要设置服务器，只要路由可达，可以指定任意的主机作为 FTP /TFTP 服务器。HTTP 升级不需要设置服务器，只要能网管 DPF-Series 设备的主机都可以为其升级，这一点类似于发送邮件时要上传一个附件。

DPF-Series 设备可以升级系统文件也可以升级配置文件。系统文件包括：

- 软代码(Firmware)：设备管理的程序
- 硬代码(Hardcode)：可以进行二次开发的 SSPP™专用芯片程序
- 驱动程序(bootrom)：引导设备启动的程序

DPF-500 以下的产品只有软代码和驱动程序，没有硬代码。DPF-2010E 以上的产品(包含 DPF-2010E/DPF-6012E)有软代码、硬代码和驱动程序。

可以同时升级软代码、硬代码和驱动，也可以只升级单个文件。升级软代码需要 1 分钟，升级硬代码要 5 分钟。升级成功后，必须重启 DPF-Series 设备才能运行新的代码。

4.2 范例：HTTP 升级

为简单起见，本手册只列举了 HTTP 的升级方法。本例中，将软件、硬件和驱动程序一起升级。首先登陆 DPF-Series 设备的网管页面。

进入**系统配置管理(SYSTEM)->系统升级(Maintenance)->系统升级(System update)，**升级方式选择 **HTTP**，点中“系统文件(System File)”，然后选择“固件 **Firmware**”、“硬代码 **Hardcode**”和“驱动 **Drivers**”，再点击“**浏览（browse）**”找到升级文件，最后再点击“升级 **update**”开始升级。如下图：

系统升级 升级 取消
升级方式 HTTP FTP/TFTP
系统升级
系统文件
固件 E:\FTP\DPF500\DPF500.bin 浏览...
驱动 浏览...
配置文件
升级病毒库 提交 取消
每天
开始时间 14 时 0 分

图1. HTTP文件升级

升级的过程中，Web 页面会有进度条提示升级的进度。升级成功后，Web 页面会返回“**Success**”，同时在事件日志里会产生升级成功的日志。

4.3 配置导出

DPF-Series 设备可以将配置导出到 PC 上，以备以后使用。

进入 **系统配置管理(SYSTEM)->当前配置(Running Settings)**，点击右上角的“另存为(**Save As)**”按钮，即可把保存当前的配置保存到 PC 上。如下：

图2. 配置导出

然后弹出以下窗口，选择文件要保存的位置，点击“**保存**”即可。



图3. 配置导出

5 设备网管

DPF-Series 设备支持 WEB 网管和 CLI 网管两种方式。为了增强系统的安全性，其中 WEB 网管的端口使用 8080，Telnet 网管的端口使用 2323。缺省情况下，两种网管的登陆用户名为 root，密码为 root*PWD。为安全起见，登陆后请及时修改密码。修改密码时，密码里面必须要包括大写字母、小写字母以及数字，例如 Abc123。

DPF-Series 设备的接口分带外接口和带内接口。OIF0 和 OIF1 为带外口，这两个口主要用于 HA 和网管。默认情况下，OIF0 为 HA 接口，OIF1 为网管接口。FE 口和 GE 口为带内数据口，用来传输业务数据。

缺省情况下，使用 DPF-Series 设备带外网管接口（OIF1 接口）来网管，其 IP 地址为 192.168.0.1/24。OIF 口不支持自动转换，和 PC 网卡相连的时候需要用交叉线连接。下面分别介绍两种网管的进入方法。

5.1 WEB 网管

可以使用 HTTP 和 HTTPS 两种方式对 DPF-Series 设备进行 WEB 网管，HTTPS 比 HTTP 具有更好的安全性。默认情况下，开启 HTTPS，这里以 HTTPS 方式为例介绍 WEB 网管。

启动 IE，在地址栏中输入 https://192.168.0.1:8080，则弹出如下对话框，提示输入用户名和密码：

登陆 [登陆]

管理员	root
密 码	********

图4. web登陆框

正确输入用户名和密码之后，进入 web 网管的主界面。

web 网管的主界面

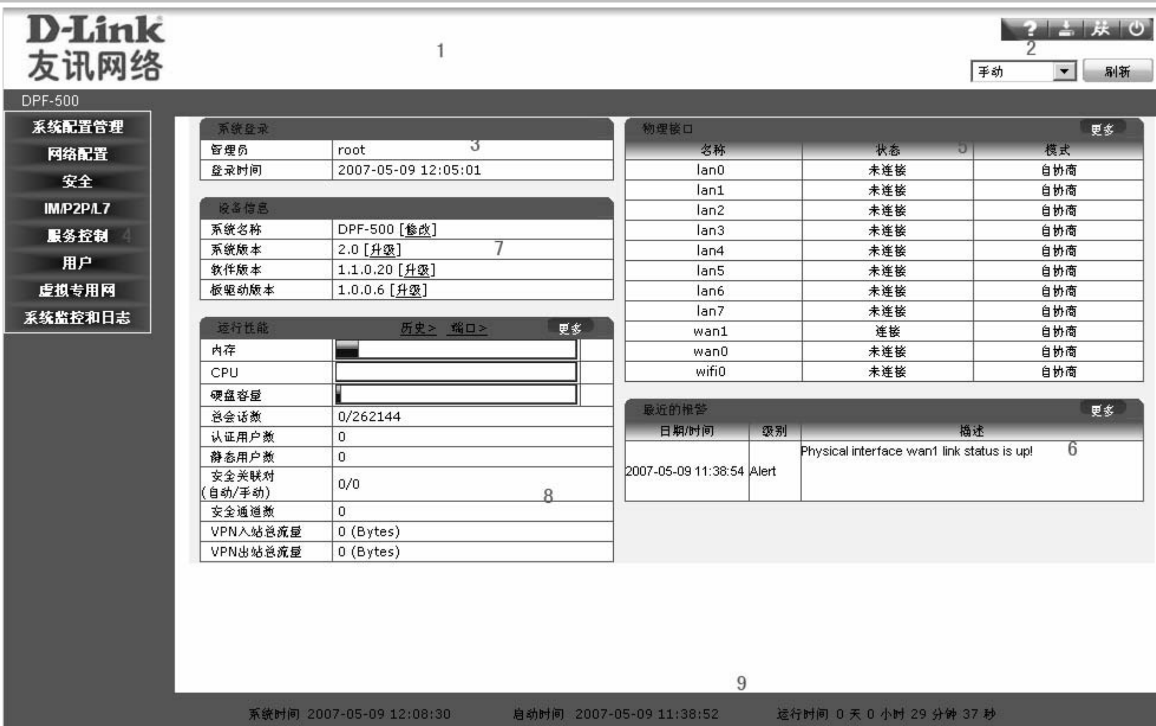


图5. web 网管的主界面

1——显示系统信息（管理员和所在系统）

2——系统功能图标，从左到右依次为系统帮助功能、保存功能、注销系统和重新启动。下方为页面刷新设置。

3——系统当前状态信息。

4——系统主菜单

5——物理接口信息，如果要查看更多的物理接口状态信息，点击 **more...**

6——最近报警信息，如果要查看更多的报警信息，点击 **more...**

7——系统设备信息，点击 **update** 可直接进入设备信息的相应版面

8——显示系统资源的使用情况，点击 **more** 查看更多信息。

9——显示 DPF-Series 设备系统时间信息、启动时间和运行时间信息

Web 历史和端口统计图

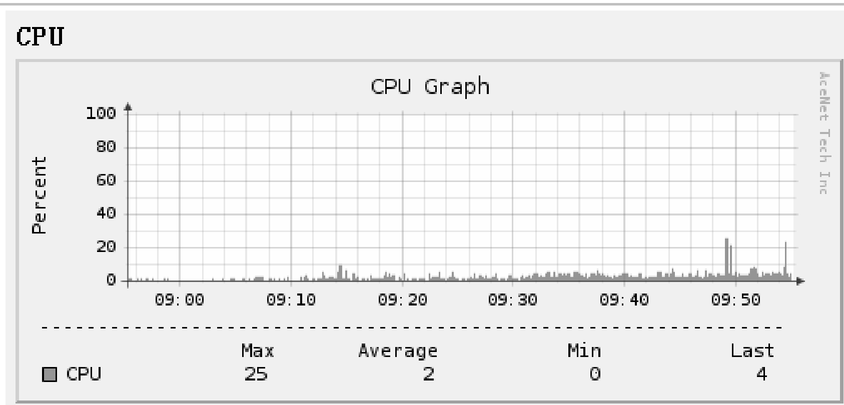
点击 Web 主页第“8”部分的 **History** 和 **Port**，可以显示 DPF-Series 设备的 CPU、内存、Session 和历史的流量统计图等等。

History 统计图

1. 系统 CPU 的利用率

   下图是周期为 1 个小时的 CPU 利用率的的历史记录图。横坐标表示时间，每小格表示 2 分钟；纵坐标表示已使用 CPU 资源的百分比，每小格为 10％。

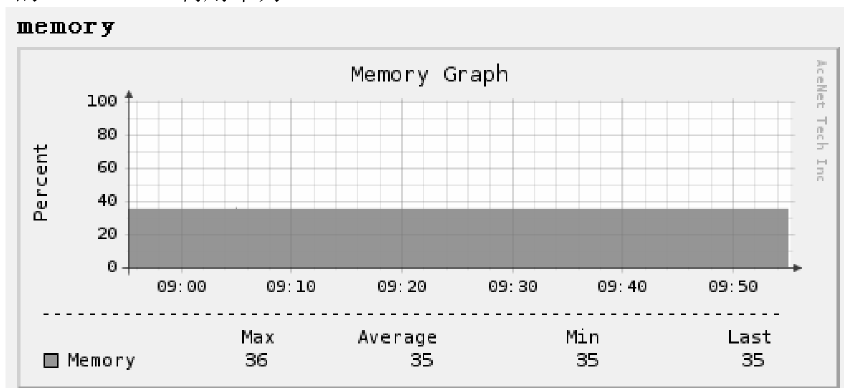
   图下部虚线表示 CPU 利用率最大时为 25％，平均利用率为 2％，最小的时候为 0%，最近的 CPU 利用率为 4%。



2. 系统内存的利用率

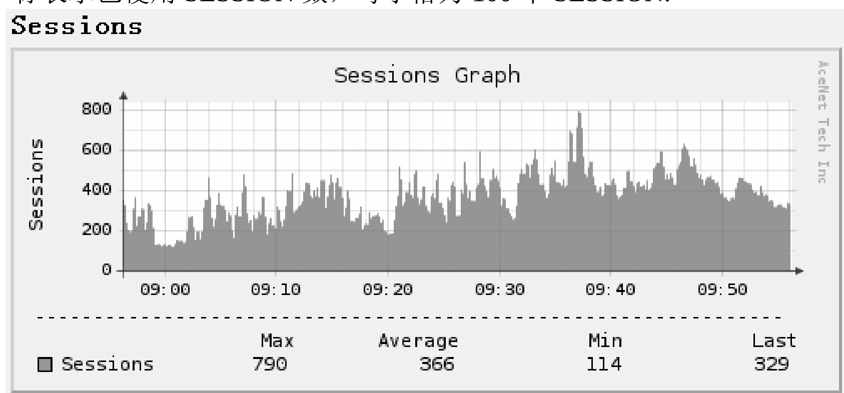
   下图是周期为 1 个小时的 MEMORY 利用率的的历史记录图。横坐标表示时间，每小格表示 2 分钟；纵坐标表示已使用 MEMORY 资源的百分比，每小格为 10%。

   图下部虚线表示 MEMORY 利用率最大时为 36%，平均利用率为 35%，最小的时候为 35%，最近的 MEMORY 利用率为 35%。



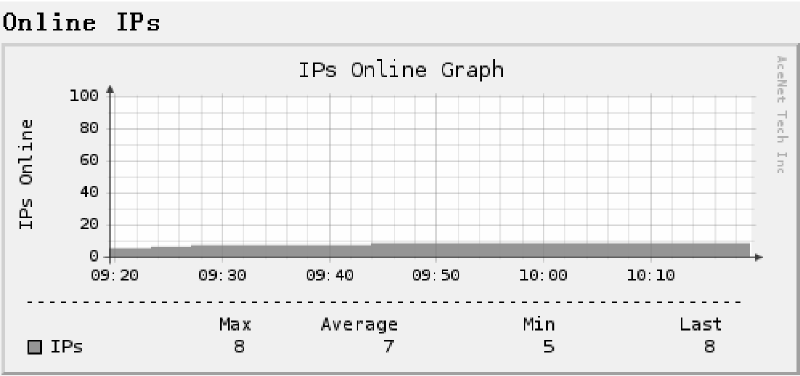
3. 系统总的 Session 统计图

   下图是周期为 1 个小时的 SESSION 数的历史记录图。横坐标表示时间，每小格表示 2 分钟；纵坐标表示已使用 SESSION 数，每小格为 100 个 SESSION.



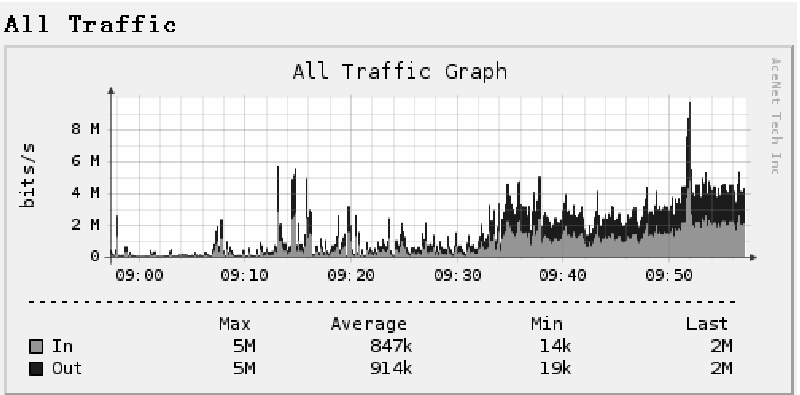
4. 在线的 IP 个数

   下图是周期为 1 个小时的在线 IP 数的的历史记录图。横坐标表示时间，每小格表示 2 分钟；纵坐标表示在线用户数，每个小格为 10 个 IP。



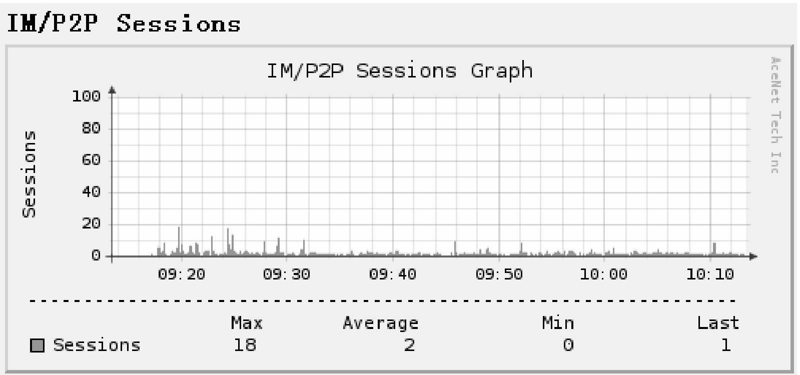
5. 系统总的流量图

   下图是周期为 1 个小时所有物理端口的流量图。横坐标表示时间，每小格表示 2 分钟；纵坐标表示流量统计值，每个小格为 1M bits/s。其中 **in** 代表所有物理端口接收流量的总和，**out** 代表所有物理端口发送流量的总和。



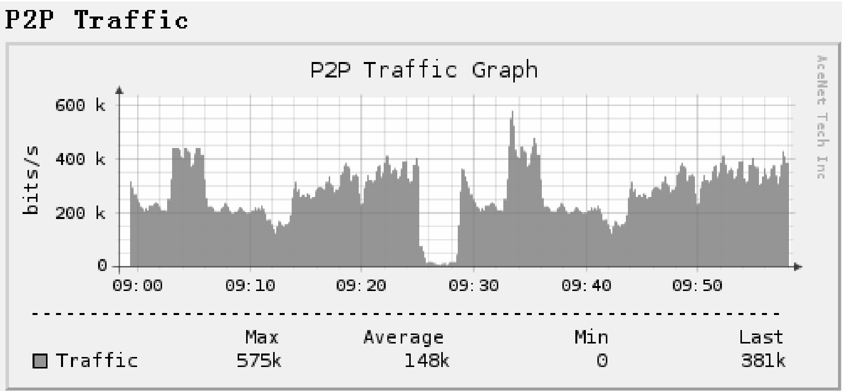
6. 系统 IM/P2P 的 Session 统计图

   下图是周期为 1 个小时的 IM/P2P 协议 SESSION 数的历史记录图。横坐标表示时间，每小格表示 2 分钟；纵坐标表示已使用 SESSION 数，每小格为 100 个 SESSION.



7. 系统 P2P 的流量统计图

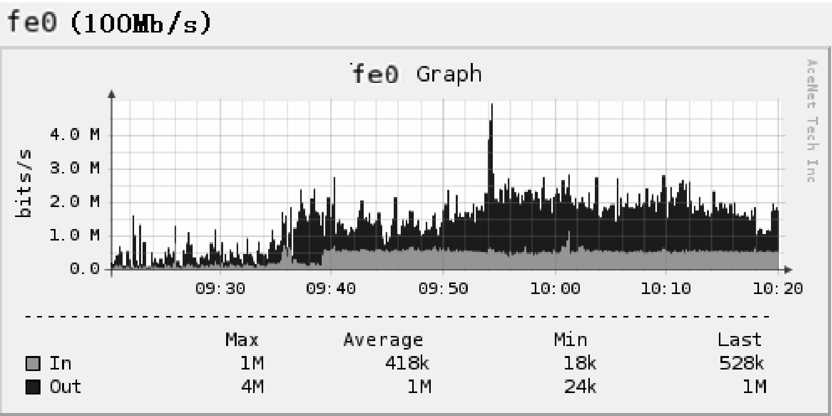
   下图为所有 P2P 协议总的流量图。横坐标表示时间，每小格表示 2 分钟；纵坐标表示 P2P 的流量值，每小格为 50K bits/s.



Port 统计图

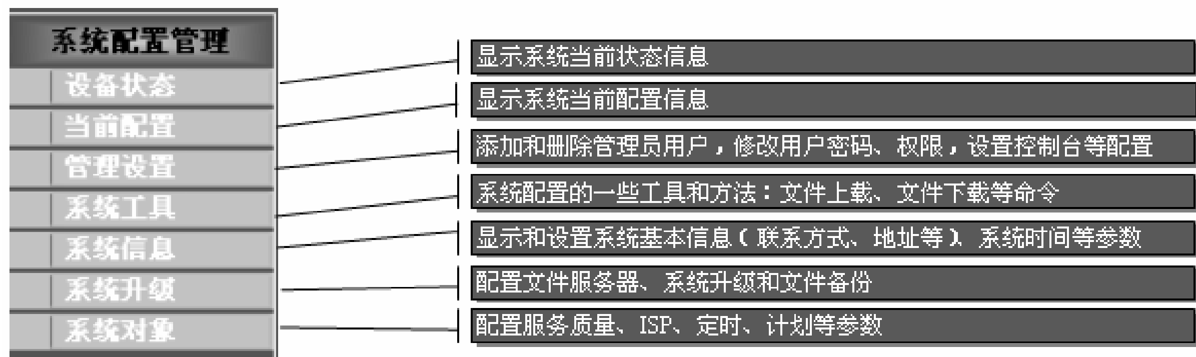
Port 统计图显示了系统每个物理接口的流量统计值，周期为 1 个小时。横坐标表示时间，每小格表示 2 分钟；纵坐标表示流量统计值，每个小格为 1M bits/s。其中 **in** 代表此物理端口接收流量的总和，**out** 代表此物理端口发送流量的总和。

为了简化篇幅，只截取了其中一个 Port 的流量图：

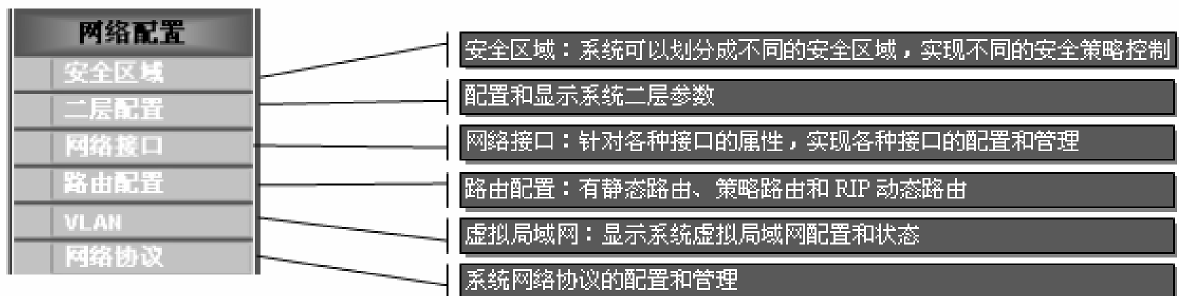


Web 网管主要功能说明

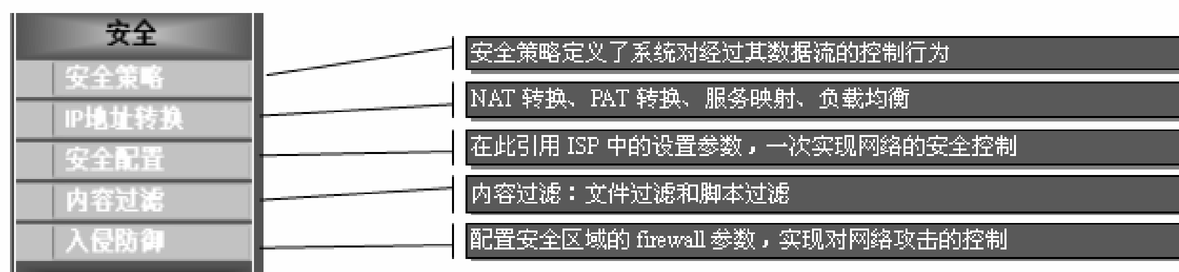
1. “系统配置管理”



2. “网络配置”



3. “安全”



4. “IM/P2P”



5. “服务控制”



6. “虚拟专用网”



7. “用户管理”

用户	
主机	配置主机信息
主机统计	主机信息统计及管理
用户管理	配置静态用户、认证用户，以及用户相关的其它信息
用户统计	用户的信息统计及管理
用户组配置	可配置认证策略、授权策略、计费策略、用户组的参数
黑名单管理	用户黑名单的配置与管理
认证服务器	Radius 服务器、LDAP 服务器的设置和管理

8. “系统监控和记录”

系统监控和日志	
监控当前连接	用户监控端口的设置
端口镜像	将某些(个)端口的流量复制到一个指定的镜像端口，以便对流量进行监控和分
日志设置	对系统日志的容量、服务器、过滤条件、EMAIL 及日志导出的设置和管理
日志显示	可以查询和清除事件日志、流量日志、监控日志和命令日志
报表设置	系统统计信息的显示和管理

5.2 CLI 网管

可以使用 telnet、ssh 和 console 三种 CLI 方式来访问 DPF-Series 设备，ssh 比其它两种方式更安全。这里介绍怎样使用 telnet 和 console 的方法。

Console 方式

首先用 Dlink 提供的**专用**的 console 线连接 DPF-Series 设备的 console 口。然后再安装如下步骤连接设备：

♦ 第一步

在开始菜单中按如下顺序点击：

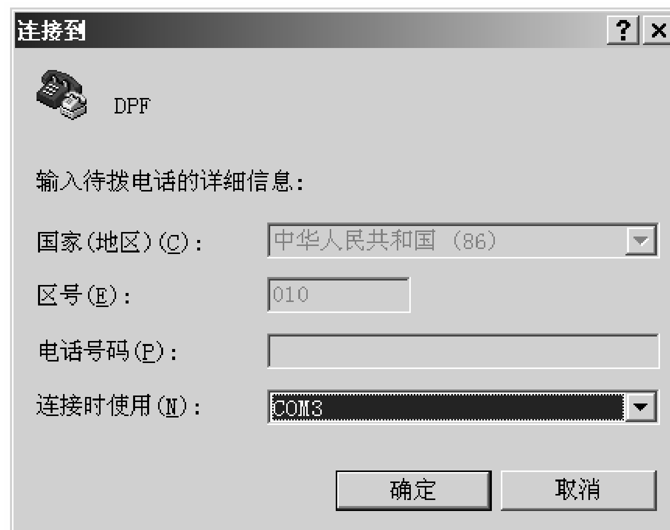
开始->程序->附件->通讯->超级终端，点击后出现如下超级终端连接描述对话框：



在名称栏中输入你要建立的连接名称，如 DPF，图标根据您的喜好选择，点击确认。

♦ 第二步

点击确认后出现如下情况：



选项“**连接时使用**”从下拉框中选择 DPF-Series 设备所链接的串口，按下确定。

♦ 第三步

按下确定后出现如下图所示情况：



配置 COM1，每秒位数选择 **115200**，数据流控制选择**无**，点击确定。

♦ 第四步

保存新建的连接 Dlink，可点击**文件**菜单下的**保存**，或点击右上角的**关闭**按钮，会出现对话框提示是否保存，选择**是**即可保存。

♦ 第五步

打开新建连接

开始->程序->附件->通讯->超级终端->DPF，或者建立一个快捷方式于桌面上。

启动 DPF-Series 设备，至此连接成功。

Telnet 方式

默认情况下，Telnet 网管方式是关闭的，所以首先要在 WEB 网管上启用。

进入 **系统配置管理(SYSTEM)->管理配置(Management)->CLI**，启用 Telnet ，如下图：

控制台CLI设置　　提交　取消

命令行启用	◉ 启用 ○ 禁用	波特率	115200
超时时间（秒）	300	每页显示行数（行）	40
SSH启用	◉ 启用 ○ 禁用		
SSH端口	2222	重新生成密钥前报文数	2147483648
Telnet启用	○ 启用 ◉ 禁用		
Telnet端口	2323	超时时间（秒）	300

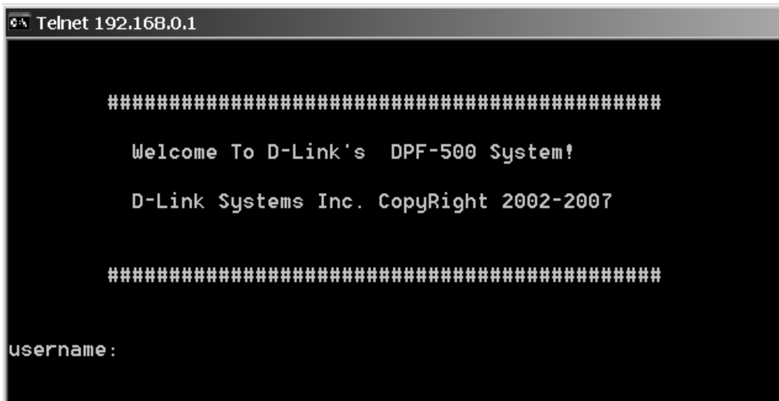
清除SSH密钥/连接　　删除　取消

清除项	□ 主机密钥 □ 所有DSA公钥 □ 当前所有SSH连接

图6. 启用 telnet

然后在 Windows 的 dos 提示符下，输入 telnet 192.168.0.1 2323，进入 CLI 网管的登陆界面。如下：

图7. CLI 登陆



正确输入用户名和密码之后进入主窗口，在主窗口输入 help 命令可以查看系统支持的主要命令：

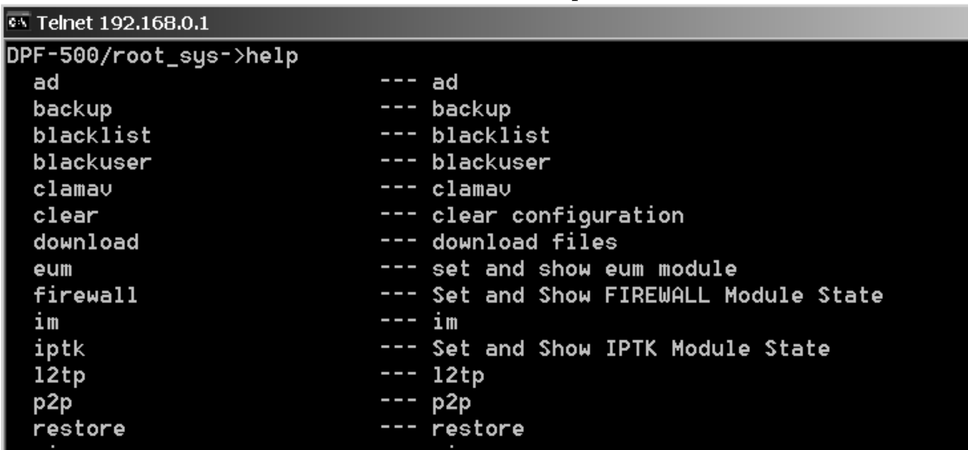


图8. “help”命令

6 物理接口

6.1 简介

DPF-Series 设备的物理接口包含带外接口和带内接口。OIF0 和 OIF1 为带外口，这两个口主要用于 HA 和网管。默认情况下，OIF0 为 HA 接口，OIF1 为网管接口。FE 口和 GE 口为带内数据口，用来传输业务数据。

DPF-Series 设备的带内物理接口有多种组合。例如 DPF-2010E 是 8 个 10M/100M 电口，再加上 2 个 10M/100M/1000M 电口或 1000M 光口。

进入 WEB 网管中的 **网络配置(NETWORK)->网络接口(Interfaces)->物理接口(Physical)** 页面可以查看所有物理接口的工作状态和配置参数。

物理接口

名称	状态	速度	模式	接收速率(Kb/s)	传输速率(Kb/s)	VLAN	物理地址	操作
共 11 条记录								
lan0	未连接	0M	自协商	0	0	1	00-18-47-09-C5-20	
lan1	未连接	0M	自协商	0	0	1	00-18-47-09-C5-21	
lan2	未连接	0M	自协商	0	0	1	00-18-47-09-C5-22	
lan3	未连接	0M	自协商	0	0	1	00-18-47-09-C5-23	
lan4	未连接	0M	自协商	0	0	1	00-18-47-09-C5-24	
lan5	未连接	0M	自协商	0	0	1	00-18-47-09-C5-25	
lan6	未连接	0M	自协商	0	0	1	00-18-47-09-C5-26	
lan7	未连接	0M	自协商	0	0	1	00-18-47-09-C5-27	
wan1	连接	100M	自协商	12	37	1	00-18-47-09-C5-28	
wan0	未连接	1000M	自协商	0	0	1	00-18-47-09-C5-29	
wifi0	未连接	0M	自协商	0	0	1	00-18-47-09-C5-2A	

图9. 物理接口

也可以点击每个物理端口对应的操作栏中的“**编辑(edit)**”按钮，来对物理接口的各个参数进行修改。

Edit Physical Interface — Apply | Cancel | Back

Name	ge1		
VLAN	1	Type	ETHER_CSMACD
Speed		Bandwidth(KB)	Both 125000
MAC Address	00-AC-E0-00-8A-C9	802.1 Priority	0
MAX Frame Size(byte)	1522	MIN Frame Size(byte)	64
Attribute	○ Sharable ◉ Dedicated	Tunnel	0
Transmitted MTU(byte)	1500	Received MTU(byte)	1500
Mode	◉ Auto ○ Full-duplex ○ Half-duplex		
Deny Ether Type	☐ ethii ☐ snap ☐ llc ☐ 802.3raw		

图10.物理接口

参数说明：

- **Mode**：物理接口的协商模式，支持自动协商、全双工和半双工
- **Speed**：当物理接口的协商模式配置成全/半双工时，可以配置该接口的工作速率，支持配置 10M/100M/1000M。在物理接口主页面中的 **Speed** 显示协商成功后的当前速率
- **Bandwidth**：指基于这个物理接口的带宽
- **R-Rate**：指物理接口当前接收数据报文的速率
- **T-Rate**：指物理接口当前发送数据报文的速率
- **Received MTU**：接收时的最大传输单元
- **Transmitted MTU**：发送时的最大传输单元

7 安全区域

在单个 DPF-Series 设备上，可以配置多个安全区，将网络分成多段，可对这些区域设置各种安全策略以满足各段的需要。但必须最少定义两个安全区，以便在网络的不同区段间分开提供基本的保护。也可以定义多个安全区，使网络安全设计具有更高的精确度。

通过安全区域的概念，把网络划分为信任区域和非信任区域两个部分，对每种区域实行不同的安全策略。同时每个区域都可以工作在路由和透明两种模式下。

缺省情况下，系统创建了 10 个安全区域。l3-in 和 l3-out 为路由模式；l2-in 和 l2-out 为透明模式。这四个安全区域主要用于数据处理，其中 l3-in 和 l2-in 具有信任属性，而 l3-out 和 l2-out 具有非信任属性。通常情况下，认为内网是安全的、可信任的，外网是不安全的、不可信任的；所以将连接内网的接口划分到信任区域，将连接外网的接口划分到非信任区域。

此外，BCAST、SELF、NULL、HA、MAN 和 HA-MAN 等六个安全区段用于系统管理，其中，SELF 安全区是系统 CPU 的区域。简单的说，就是报文是由 CPU 发起，则源安全区就是 SELF；或者报文是发给 CPU 的，则目的安全区就是 SELF。换句话说，就是报文 **源/目的** IP 地址是 DPF-Series 设备自身的 IP 地址，此时 **源/目的** 安全区就是 SELF。设备自身的 IP 地址包括 Layer 2 IP 和 **路由/NAT** 模式下的虚拟接口的 IP 地址。

默认的安全区如下：

安全区域 新增

序号	名称	信任	模式	操作
共 7 条记录				
3	l3-in	信任	路由模式	
4	l3-out	不信任	路由模式	
5	l2-in	信任	透明模式	
6	l2-out	不信任	透明模式	
126	BCAST	不信任	N/A	
127	SELF	不信任	N/A	
128	NULL	不信任	N/A	

图11.安全区域

可以使用默认的安全区域，也可以按需新建安全区域。进入**网络配置(NETWORK)->安全区域(Zones) ->新增(CreateNew)**，创建一个新的安全区域。为这个安全区命名为 meili，选择路由模式和信任属性。如下：

新增安全区域 提交 取消 返回

名称	meili		
模式	路由模式	信任	信任

图12.安全区域

8 虚拟接口

8.1 简介

DPF-Series 设备支持虚拟接口的概念，通过 vlan 可以在每个物理接口上创建 4094 个虚拟接口。也就是说，vif 是由物理接口和 Vlan 两个关键字组合而成。例如，FE2+vlan2 可以组成一个 vif（命名为 vif-h），而 FE2+vlan3 也可以组成一个 vif（命名为 vif-y）。

每个虚拟接口都必须属于一个安全区域，因此虚拟接口继承了它所在的安全区域的工作属性。包括**路由/透明**模式和**信任/非信任**属性等。例如，把 vif1 绑定到 l2-in，则 vif1 就是透明模式，属于信任域。而把 vif1 绑定到 l3-out，则 vif1 就是路由模式，且属于非信任域。

透明模式的虚拟接口没有 IP 地址。路由模式的虚拟接口必须配置 IP 地址，如果没有配置 IP 地址，则这个接口是无效的，每个虚拟接口可以配置最多 8 个 IP 地址。缺省情况下，所有的虚拟接口都工作在透明模式，可以修改虚拟接口关联的安全区域来改变它的模式。下图描述了将物理接口、虚拟接口和安全区域之间的关系：

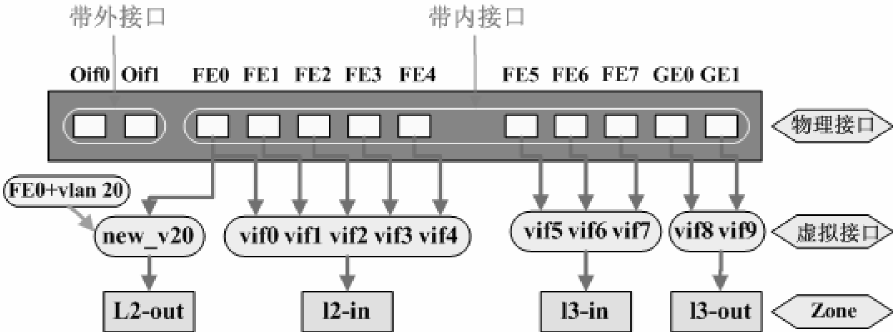


图13.物理接口-虚拟接口-zone 关系图

虚拟接口　　新增

共 9 条记录 当前第 1 页

序号	名称	物理接口/汇聚口	VLAN	IP地址1/掩码	工作模式	区域	有效	操作
1	vif0	lan0	1		透明模式	l2-in	是	
2	vif1	lan1	1		透明模式	l2-in	是	
3	vif2	lan2	1		透明模式	l2-in	是	
4	vif3	lan3	1		透明模式	l2-in	是	
5	vif4	lan4	1		透明模式	l2-in	是	
6	vif5	lan5	1		透明模式	l2-in	是	
7	vif6	lan6	1		透明模式	l2-in	是	
8	vif7	lan7	1		透明模式	l2-in	是	
9	vif9	wan0	1		透明模式	l2-in	是	

8.2 VIF 参数说明

每个虚拟接口具有自己的属性，包括安全属性、tag/untag 和 IP 地址等。如图：

虚拟接口 | 物理接口 | 管理接口 | 二层接口 | 汇聚接口

修改虚拟接口　　提交 取消 返回

虚接口名称	vif0	物理口/汇聚接口	lan0	有效	⊙是 ○否
VLAN	1	区域	l2-in		
加VLAN标签	☐	工作模式	透明模式		
报文允许	☐ web ☐ telnet ☐ ssh ☐ ping ☐ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

下面分别介绍一些重要的参数：

- PHY-IF/Trunk：此虚拟接口关联的物理接口或者 trunk 接口
- VLAN：此虚拟接口关联的 VLAN ID
- Zone：此虚拟接口关联的 Zone
- Valid：此虚拟接口是有效的还是无效的
- Tagged：此虚拟接口是否带 Vlan 标记
- Permit：在虚拟接口上也有对一些特殊报文是否允许的开关，可以允许（或者拒绝）web、ping、telnet、ssh 和 snmp 报文。这些报文是指到 CPU 的，即目的是到 SELF 安全区的。如果允许 ping，则可以通过此接口 ping 到 DPF-Series 设备；如果允许 web，则可以通过此接口连接 DPF-Series 设备的 web 网管；其它报文类型类似。如果拒绝某类型的报文，当 vif 收到这种类型的，并且是到 CPU 的报文，则会丢弃它。
- Auth：此接口的一些认证方式。比如要使用 web 认证，就需要在此接口上启用 **web Auth**

8.3 新建 VIF 范例

1. 新建透明模式的 vif

   进入**网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)->新增(CreateNew)**，新建一个透明模式的 vif，名字为 vif-x，物理接口 Lan0、VLAN 100、untagged、属于 l2-in。

新增虚拟接口					提交 取消 返回
虚接口名称	vif-x	物理接口/汇聚口	lan0		
VLAN	100	区域	l2-in		
加VLAN标签	☐				
有效	⦿ 是 ○ 否				
报文允许	☐ web ☐ telnet ☐ ssh ☐ ping ☐ snmp ☐ 全部				
认证开关	☐ web认证 ☐ 设备认证				

图14.vif

2. 新建路由模式的 vif

   进入**网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)->新增(CreateNew)**，新建一个路由模式的 vif，名字为 vif-r，物理接口 Lan0、VLAN 60、tagged、IP 为 1.1.1.1/24，属于 l3-in。

新增虚拟接口					提交 取消 返回
虚接口名称	vif-r	物理接口/汇聚口	lan0		
VLAN	60	区域	l3-in		
加VLAN标签	☐				
有效	⦿ 是 ○ 否				
报文允许	☐ web ☐ telnet ☐ ssh ☐ ping ☐ snmp ☐ 全部				
认证开关	☐ web认证 ☐ 设备认证				

图15.vif

9 透明模式

9.1 简介

接口为透明模式时，DPF-Series 设备过滤通过防火墙的封包，而不会修改 IP 封包包头中的任何源或者目的信息。所有接口运行起来都像是同一网络中的一部分，而 DPF-Series 设备的作用更像是第 2 层交换机或桥接器。在透明模式下，DPF-Series 设备对于用户来说是 “透明”的，不需要进行任何路由配置以及网络拓扑变化，同时能完成外部网络的安全防御、链路可靠性保证，以及内部网络管理控制、统计和监控功能。

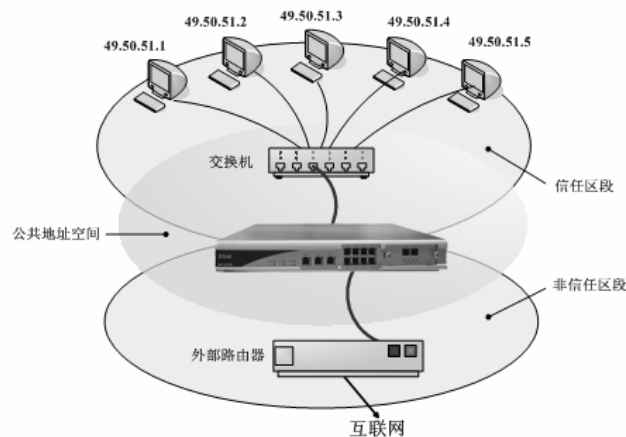


图16.透明模式

- **二层接口 ip**

  所有透明模式的接口共用一个 ip 地址，即 l2-if IP 地址，在缺省情况下是 10.1.1.1/24。可以修改 l2-if 的地址或者为其增加多个第二 IP 地址。用户可以利用这些地址进行网管和监控 DPF-Series 设备。

- **区段**

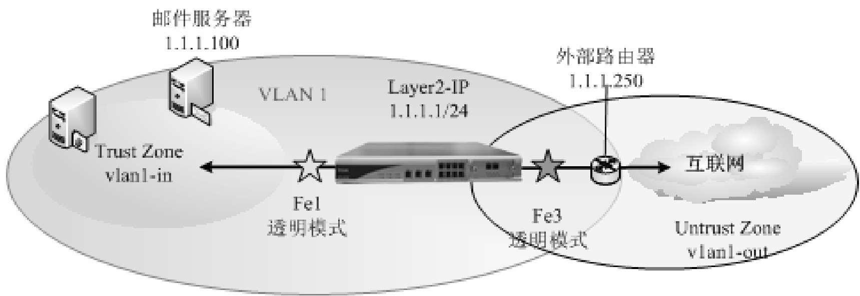
  缺省情况下，DPF-Series 设备有两个区段是透明模式的，一个是 Trust 区段的 l2-in，一个是 Untrust 的 l2-out。也可以自己新建透明模式的区段。接口绑定透明模式的区段时，此接口就成为透明模式的接口。

- **Vlan**

  缺省情况下，所有的接口都工作于透明模式，属于 vlan 1，也可以选定物理端口和 vlan 来新建虚拟接口。透明模式下，同一 vlan 之间的接口可以通信。

9.2 范例

以下范例说明了处于透明模式的受 DPF-Series 设备保护的单独 LAN 的基本配置。策略允许 Vlan1-in 区段中所有主机的外向信息流、邮件服务器的内向 POP3 服务，以及 FTP 服务器的内向 FTP 服务。为了提高管理信息流的安全性，缺省情况下，将 Web 管理的 HTTP 端口号从 80 改为 8080，将 CLI 管理的 Telnet 端口号从 23 改为 2323。使用 l2-if IP 地址 1.1.1.1/24 来管理 DPF-Series 设备。Vlan1-in 区段中所有主机的缺省网关是 1.1.1.250。



本例中，不使用系统默认的 zone，而是新建两个 zone（vlan1-in 和 vlan1-out）。采用默认 VLAN 1。

CLI

1. l2-if

   set l2-if ip 1.1.1.1 netmask 255.255.255.0

2. 区段

   set zone new vlan1-in transparent trust in-vr
   set zone new vlan1-out transparent untrust in-vr

3. 接口

   set vif vif1filters enable web,telnet,ping
   set vif vif1zone vlan1-in
   set vif vif3 zone vlan1-out

4. 策略

   firewall set policy from vlan1-in to vlan1-out src-addr ANY dst-addr ANY service ANY action permit status enable
   firewall set policy from vlan1-out to vlan1-in src-addr ANY dst-addr 1.1.1.50service FTP action permit status enable
   firewall set policy from vlan1-out to vlan1-in src-addr ANY dst-addr 1.1.1.100 service POP3 action permit status enable

WEB 配置

WEB 的配置与 CLI 的配置相对应：

1. l2-if

   进入 **网络配置(NETWORK)->网络接口(Interfaces)->Layer2->新增(Create New)**，添加 IP 地址为 1.1.1.1/24

新增IP		提交 取消 返回	
IP地址		子网掩码	

图17.l2-if

2. 区段

   进入 **网络配置(NETWORK)->安全区域(Zones)->新增(Create New)**，添加一个透明模式的 zone，名为 vlan1-in，属于信任域。

新增安全区域		提交 取消 返回	
名称	vlan1-in		
模式	透明模式	信任	信任

图18.区段

同样添加一个名为 vlan1-out 的 zone，透明模式，属于非信任域。如下图:

新增安全区域			提交 取消 返回
名称	vlan1-out		
模式	透明模式	信任	信任

图19.区段

3. 接口

进入 **网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)->vif1->edit**，这里要选择允许 ping，telnet，web 管理，然后 zone 选择为 vlan1-in

新增虚拟接口			提交 取消 返回
虚接口名称	VIF1	物理接口/汇聚口	lan1
VLAN		区域	LAN-IN
加VLAN标签	☐		
有效	○ 是 ⦿ 否		
报文允许	☐ web ☐ telnet ☐ ssh ☐ ping ☐ snmp ☐ 全部		
认证开关	☐ web认证 ☐ 设备认证		
	IP 地址	子网掩码	

图20.接口设置接口设置

再编辑 vif3，zone 选择 vlan1-out。如下：

新增虚拟接口			提交 取消 返回
虚接口名称	VIF3	物理接口/汇聚口	lan3
VLAN		区域	LAN-out
加VLAN标签	☐		
有效	○ 是 ⦿ 否		
报文允许	☐ web ☐ telnet ☐ ssh ☐ ping ☐ snmp ☐ 全部		
认证开关	☐ web认证 ☐ 设备认证		
	IP 地址	子网掩码	

图21.接口设置

4. 策略

进入 **安全(SECURITY)-> 安全策略(Policies)->新增(Create New)**，这里选择从源区段 any 到目的区段 any，策略为 permit all

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 之前 ⦿ 最后		
安全区			
源安全区	ANY	目的安全区	ANY
地址/用户/地址簿			
	⦿ 源 地址 ○ 用户 ○ 地址簿		
	⦿ 目的地址 ○ 用户 ○ 地址簿		
动作	PERMIT	服务	ANY
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☐ 显示高级	

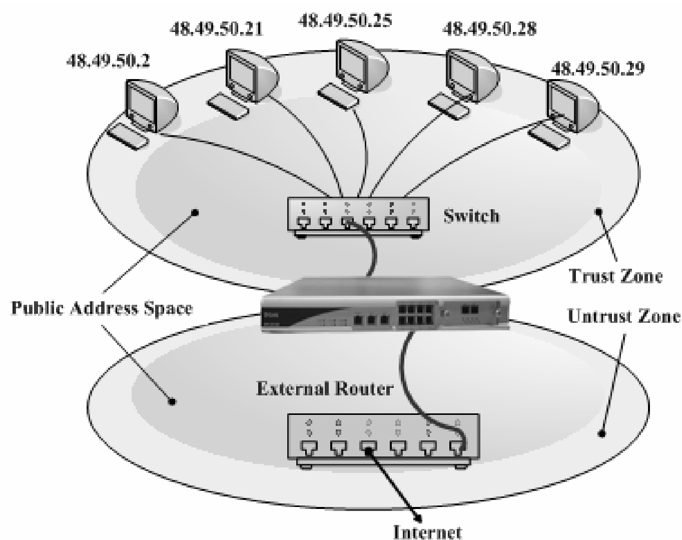
图22.建立策略

10 路由模式

10.1 简介

接口为路由模式时，DPF-Series 设备在不同区段间转发信息流时不执行 NAT。 与透明模式不同，每个区段内的接口可以工作在不同的子网中。此模式下 DPF-Series 设备工作类似一个路由器，可以进行路由拓扑构造。

为了适应特殊的需求，不同的路由模式接口可以拥有相同的 IP 地址，但是不能拥有同一子网中不同 IP 地址。例如，vif1 和 vif2 的 IP 地址可以都配置为 1.1.1.5/24，但是不能 vif1 的 IP 配置为 1.1.1.6/24，而 vif2 的 IP 配置为 1.1.1.8/24。



◆ **区段**

缺省情况下，DPF-Series 设备有两个区段是路由模式的，一个是 Trust 区段的 l3-in，一个是 Untrust 的 l3-out。也可以自己新建路由模式的区段。接口绑定路由模式的区段时，此接口就成为路由模式的接口。

◆ **接口设置**

可以改变缺省情况下的虚拟接口的模式为路由模式，也可以选定需要的物理端口和 vlan 来新建虚拟接口，模式选择为路由模式。

10.2 范例 1

以下范例说明了 Trust 区段中有单独子网的 LAN 的简单配置。策略允许 Trust 区段中所有主机的外向信息流和 FTP 服务器的内向邮件。Trust 区段 LAN 中的主机具有公共 IP 地址，所有安全区都在 in-vr 虚拟路由器中。Trust 区段中所有主机的缺省网关是 12.12.12.1。



CLI

1. 接口
```
set vif vif1 zone l3-in
set vif vif3 zone l3-out
set vif vif1 ip 12.12.12.1 netmask 255.255.255.0
set vif vif3 ip 1.1.1.1 netmask 255.255.255.0
set vif vif1 filters enable web,telnet,ping
set vif vif3 filters enable web,telnet,ping
```
2. 路由
```
set route ip 0.0.0.0 0.0.0.0 1.1.1.250
```
3. 策略
```
firewall set policy from l3-in to l3-out src-addr ANY dst-addr ANY service ANY action permit status enable
firewall set policy from l3-out to l3-in src-addr ANY dst-addr 12.12.12.5 service FTP action permit status enable
```

WEB 配置

WEB 的配置与 CLI 的配置相对应：

1. 接口

路由模式接口的 IP 地址配置： 进入 **网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)->Vif1**，修改 zone 为 l3-in，使其成为路由模式的接口。

修改虚拟接口 提交 取消 返回

虚接口名称	vif1	物理口/汇聚接口	lan1	有效	◉ 是 ○ 否
VLAN	1	区域	l3-in		
加VLAN标签	☐	工作模式	透明模式		
报文允许	☐ web ☐ telnet ☐ ssh ☐ ping ☐ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

图1. 接口配置

同理修改 vif3, 如下：

修改虚拟接口 提交 取消 返回

虚接口名称	vif3	物理口/汇聚接口	lan3	有效	◉ 是 ○ 否
VLAN	1	区域	l3-out		
加VLAN标签	☐	工作模式	透明模式		
报文允许	☐ web ☐ telnet ☐ ssh ☐ ping ☐ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

图2. 接口配置

为 vif1 配置 IP 地址：12.12.12.1/24,如下：

新增IP		提交 取消 返回	
名称	wan1		
IP地址	12.12.12.1	子网掩码	255.255.255.0

图3. 配置 IP

为 vif3 配置 IP 地址：1.1.1.1/24，如下：

新增IP		提交 取消 返回	
名称	wan1		
IP地址	1.1.1.1	子网掩码	255.255.255.0

图4. 配置 IP

2. 路由

DPF-Series 设备支持静态路由、策略路由和 RIP 动态路由，这里使用静态路由。
进入 网络配置(NETWORK)->路由配置(Routing)->网络路由(Static Routing)->新增(Create New)，添加一条到 1.1.1.250 的静态路由：

新增网络路由表		提交 取消 返回	
IP地址	0.0.0.0	子网掩码	0.0.0.0
网关/ISP	1.1.1.250		
*IP地址 0.0.0.0 掩码 0.0.0.0 代表缺省路由			

图5. 路由

3. 策略

进入 **安全(SECURITY)->安全策略(Policies)->新增(Create New)**，配置一条从源安全区段 l3-in 到目的安全区段 l3-out， permit all 的策略。

新增安全策略		提交 取消 返回	
位置	○ 置顶 ○ 在 ____ 之前 ⦿ 最后		
安全区			
源安全区	l3-in	目的安全区	l3-out
地址/用户/地址簿			
⦿ 源 地址 ○ 用户 ○ 地址簿			
⦿ 目的地址 ○ 用户 ○ 地址簿			
动作	PERMIT	服务	ANY
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☐ 显示高级	

图6. 策略

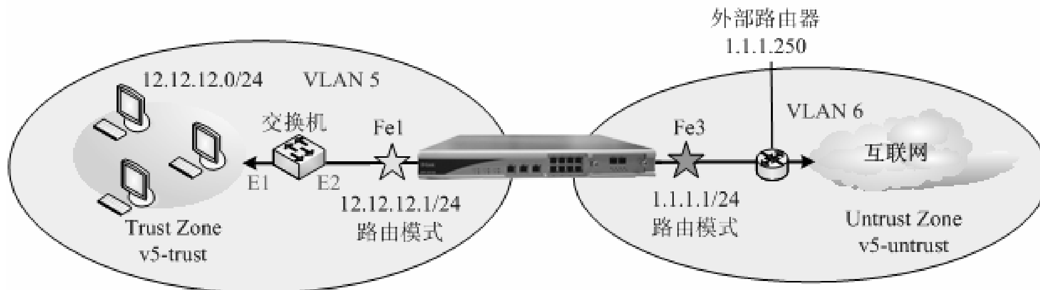
然后配置一条从源安全区段 l3-out 到目的安全区段 l3-in，目的 IP 是 12.12.12.5，服务选择 FTP 的策略。

新增安全策略		提交 取消 返回	
位置	○ 置顶 ○ 在 ____ 之前 ⦿ 最后		
安全区			
源安全区	ANY	目的安全区	ANY
地址/用户/地址簿			
⦿ 源 地址 ○ 用户 ○ 地址簿			
⦿ 目的地址 ○ 用户 ○ 地址簿		12.12.12.5	
动作	PERMIT	服务	ANY
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☐ 显示高级	

图7. 策略

10.3 范例 2

某个工作组通过一个二层的交换机连接到工作于路由模式的 DPF-Series 设备上。策略允许 Trust 区段中所有主机的外向信息流。所有安全区都在 in-vr 虚拟路由器中。Trust 区段中所有主机的缺省网关是 12.12.12.1。



本例中，不使用系统默认的 zone，而是新建两个 zone（v5-trust 和 v5-untrust）。也不采用默认 VLAN，使用新建的两个 VLAN (VLAN 5 和 VLAN 6)。所以要新建两个虚拟接口(fe1-v5 和 fe3-v6)，fe1-v5 带上 vlan-tag，fe3-v5 为 untag。交换机的 E1 和 E2 端口都属于 VLAN 5，并且 E2 带上 vlan-tag。

CLI

1. 区段
   set zone new v5-trust router trust in-vr
   set zone new v5-untrust router untrust in-vr
2. 接口
   set vif new fe1-v5 phy-if fe1 5
   set vif fe1-v5 vlan-tag enable
   set vif new fe3-v6 phy-if fe1 6
   set vif fe1-v5 zone v5-trust
   set vif fe3-v5 zone v5-untrust
   set vif fe1-v5 ip 12.12.12.1 netmask 255.255.255.0
   set vif fe3-v5 ip 1.1.1.1 netmask 255.255.255.0
   set vif fe1-v5 filters enable web,telnet,ping
   set vif fe3-v5 filters enable web,telnet,ping
3. vlan-port-mapping
   set vlan-port-mapping phy-if fe1 vid 5 8021p 0
   set vlan-port-mapping phy-if fe3 vid 6 8021p 0
4. 路由
   set route ip 0.0.0.0 0.0.0.0 1.1.1.250
5. 策略
   firewall set policy from v5-trust to v5-untrust src-addr ANY dst-addr ANY service ANY action permit status enable

注意： 通过新建虚拟接口(fe1-v5 和 fe3-v6)来增加 VLAN 5 和 VLAN 6，使得 VLAN 5 中包含 FE1，使得 VLAN 6 中包含 FE3。

WEB 配置

WEB 的配置与 CLI 的配置相对应：

1. 区段

进入 **网络配置(NETWORK)->安全区域(Zones)->新增(Create New)**，添加一个路由模式的 zone，名为 v5-trust，属于信任域。

新增安全区域			提交 取消 返回
名称	v5-trust		
模式	路由模式	信任	信任

图8. 区段配置

再添加一个名为 v5-untrust 的 zone，路由模式，属于非信任域。

新增安全区域			提交 取消 返回
名称	v5-untrust		
模式	路由模式	信任	不信任

图9. 区段配置

2. 接口

进入 **网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)->新增(Create New)**，新增虚拟接口 fe1-v5，物理接口选择 FE1，VLAN 输入 5，区域选择 v5-trust，允许 ping、telnet、web 管理，带上 vlan-tag，IP 地址为 12.12.12.1/24。

新增虚拟接口			提交 取消 返回
虚接口名称	fe1-v5	物理接口/汇聚口	lan1
VLAN	5	区域	l3-in
加VLAN标签	☐		
有效	⦿ 是 ○ 否		
报文允许	☑ web ☑ telnet ☐ ssh ☑ ping ☐ snmp ☐ 全部		
认证开关	☐ web认证 ☐ 设备认证		
	IP 地址 12.12.12.1	子网掩码 255.255.255.0	

图10.接口配置

同理新增虚拟接口 fe3-v6，物理接口选择 FE3，VLAN 输入 6，区域选择 v5-untrust，允许 ping、telnet、web 管理，IP 地址为 1.1.1.1/24。

新增虚拟接口			提交 取消 返回
虚接口名称	fe3-v6	物理接口/汇聚口	lan3
VLAN	5	区域	l3-in
加VLAN标签	☐		
有效	⦿ 是 ○ 否		
报文允许	☑ web ☑ telnet ☐ ssh ☑ ping ☐ snmp ☐ 全部		
认证开关	☐ web认证 ☐ 设备认证		
	IP 地址 1.1.1.1	子网掩码 255.255.255.0	

图11.接口配置

3. vlan-port-mapping

进入 **网络配置(NETWORK)-> VLAN->VLAN Table**，可以看到所有 VLAN：

"T" 一带VLAN TAG 的成员 "U" 一不带VLAN TAG 的成员

序号	VLAN	Port Members									
		LAN0	LAN1	LAN2	LAN3	LAN4	LAN5	LAN6	LAN7	WAN1	WAN
共 1 条记录 当前第 1 页 "T":Tagged "U":Un-tagged											
1	1	U	U	U	U	U	U	U	U		

图12.vlan配置

进入 **网络配置(NETWORK)->VLAN->基于端口的 VLAN->lan0->edit**，为 lan0 配置 default vlan，从下拉框里选择 5 。

基于端口的VLAN映射修改			提交 取消 返回
物理接口/汇聚口	lan0	VLAN	5

图13.Port Based VLAN 配置

4. 路由

进入 **网络配置(NETWORK)->路由配置(Routing)->网络路由(Static Routing)->新增(Create New)，**添加一条到 1.1.1.250 的静态路由。

新增网络路由表			提交 取消 返回
IP地址	0.0.0.0	子网掩码	0.0.0.0
网关/ISP	1.1.1.250		
*IP地址 0.0.0.0 掩码 0.0.0.0 代表缺省路由			

图14.路由

5. 策略

进入 **安全(SECURITY)->安全策略(Policies)->新增(Create New)**，配置一条从源安全区段 v5-trust 到目的安全区段 v5-untrust，permit all 的策略。

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 ____ 之前 ⊙ 最后		
安全区			
源安全区	v5-trust	目的安全区	v5-untrust
地址/用户/地址簿			
⊙ 源 地址 ○ 用户 ○ 地址簿			
⊙ 目的地址 ○ 用户 ○ 地址簿			
动作	PERMIT	服务	ANY
日志	☐ log		
防病毒	☐ 防病毒		
使能	⊙ 启用 ○ 禁用	☐ 显示高级	

图15.策略

11 路由

11.1 ISP 简介

ISP(Internet Service Provider)，叫做因特尔网服务提供商，例如电信、联通、网通等运营商。当我们向电信申请一条线路时，电信会给我们指定一个网关 IP 地址或者 ADSL 帐号，然后我们通过这个 IP 地址或者 ADSL 帐号接入互联网。在 DPF-Series 设备上，我们将 ISP 定义为网关 IP 地址或者 ADSL 帐号。所以 ISP 有两种类型：IP 和 PPPoE(ADSL 拨号)。DPF2010E/6012E 系列只支持类型为 IP 地址的 ISP，DPF-500 支持类型为 IP 和 PPPoE 的 ISP，下面来具体说明一下 ISP 的配置。

1. IP 类型的 ISP 配置

新增ISP	提交 取消 返回		
名称	isp_telcom		
注释			
类型	◉ IP ○ PPPoE		
IP地址	58.60.231.113	DNS IP地址1	202.96.128.68
DNS IP地址2	202.96.134.133	DNS IP地址3	202.96.154.8
侦测允许	☑		
侦测目标	www.google.com		

图16. IP 类型的 ISP

参数说明：

- **IP Address**：运营商提供的网关 IP
- **DNS IP Addres**：当地的 DNS 地址，DNS IP Addres1 是主 DNS，DNS IP Addres2 和 DNS IP Addres3 是备份 DNS
- **Track enable**：是否对 ISP 进行健康侦探测
- **Track Target**：侦测的目标 URL，不输入任何值时是侦测 www.sina.com

2. PPPoE 类型的 ISP 配置

新增ISP	提交 取消 返回		
名称	pppoe1		
注释			
类型	○ IP ◉ PPPoE		
用户名	szace941@163.gd	密码	96959488
接口	vif1		
侦测允许	☑		
侦测目标	www.sina.com		

图17. PPPoE 类型的 ISP

参数说明：

- **Type**：IP 或者 PPPoE
- **Username** 和 **Password**：运营商提供帐号
- **DNS IP Addres**：当地的 DNS 地址，DNS IP Addres1 是主 DNS，DNS IP Addres2 和 DNS IP Addres3 是备份 DNS
- **Interface**：DPF-Series 设备通过哪个虚拟接口拨号，这个接口必须是属于 untrust zone
- **Track enable**：是否对 ISP 进行健康侦探测
- **Track Target**：侦测的目标 URL，不输入任何值时是侦测 www.sina.com

备注：ISP 的健康侦测是通过 **DNS IP Addres** 地址去解析 **Track Target**(目标 URL)，如果可以解析出

来，则说明这条 ISP 是健康的。

11.2 路由简介

DPF-Series 设备支持静态路由、动态路由(RIP)和策略路由。本章主要介绍静态路由和策略路由。其中静态路由又分为两种：

- 普通型：下一跳是一个明确的 IP 地址（如 1.1.1.1），其配置和传统的路由器、三层交换机的静态路由配置方法相同。
- 高级型：下一跳是一个已定义好的 ISP 名称（如 isp_telcom），配置高级型静态路由需要先定义 ISP。

静态路由的配置：

1. 普通型静态路由

新增网络路由表			提交 取消 返回
IP地址	68.21.25.0	子网掩码	255.255.255.0
网关/ISP	1.1.1.1		
*IP地址 0.0.0.0 掩码 0.0.0.0 代表缺省路由			

图18. 普通型静态路由

2. 高级型静态路由

新增网络路由表			提交 取消 返回
IP地址	58.32.0.0	子网掩码	255.248.0.0
网关/ISP	isp_telcom		
*IP地址 0.0.0.0 掩码 0.0.0.0 代表缺省路由			

图19.高级型静态路由

参数说明：

- **IP Address**：路由的目的网络地址
- **Netmask**：目的网络地址的掩码
- **Gateway/ISP**：路由的下一跳。如果是一个确定的 IP 地址(如 1.1.1.1)，就是普通型的静态路由；如果是一个已定义好的 ISP 名称（如 isp_telcom），此路由就是高级型的静态路由

路由的优先级 依次排列如下：
高级型的静态路由>策略路由>普通型的静态路由＝动态路由

当数据包需要 DPF-Series 设备路由时，DPF-Series 设备首先根据预先设定的高级型静态路由对数据包进行匹配，如果匹配到高级静态路由，就根据该条路由指定的 ISP 进行转发；如果没有匹配到任何高级路由，就匹配策略路由，如果匹配到一条策略路由，就根据该条路由指定的 ISP 进行转发；如果没有匹配到任何策略路由，就使用普通型静态路由(或者动态路由)表中的路由转发数据包；如果还是没有匹配到任何路由，就丢弃该数据包。

11.3 策略路由

基于策略的路由比传统路由强，使用更灵活，它使网络管理者不仅能够根据目的地址而且能够根据源安全区、源 IP 地址、协议类型以及目的端口号来选择转发路径。策略路由提供了这样一种机制：根据网络管理者制定的标准来进行报文的转发，这种选择的自由性是很需要的。

DPF-Series 设备还支持链路备份和负载均衡。可以将多个 ISP 配置到一个 ISP 池里。如下：

策略路由　新增　清除

序号	源安全区	源地址	目的地址	协议	端口	ISP/ISP池	操作

共 0 条记录

图20.　　isp pool

参数说明：

- **ISP Name**：ISP 成员的名称
- **Priority：**ISP 优先级
- **Balance**：某个 ISP 在 ISP Pool 中占的 Balance 比例，同一优先级的 ISP，Balance 总和必须为 8。

配置策略路由时，网络管理员可以指定出口是某个具体的 ISP 或者 ISP 池。在 ISP 池中，可以指定 ISP 成员的优先级来实现链路备份和负载均衡。如果 ISP 池中 ISP 成员的优先级相同，则流量在多个 ISP 之间随机均衡；如果其中一个失效，则在剩下的 ISP 成员之间均衡。如果 ISP 成员的优先级不同，则选择高优先级的 ISP 作为路由出口，当高优先级的 ISP 失效后，才启用低优先级的 ISP。如果高优先级的 ISP 故障恢复，则路由出口重新选择高优先级的 ISP。下图就是典型的策略路由的网络拓扑。



策略路由的优先级为：

ID 号小的优先级高，当进行策略路由的查找时，找到第一个匹配的路由则停止查找。

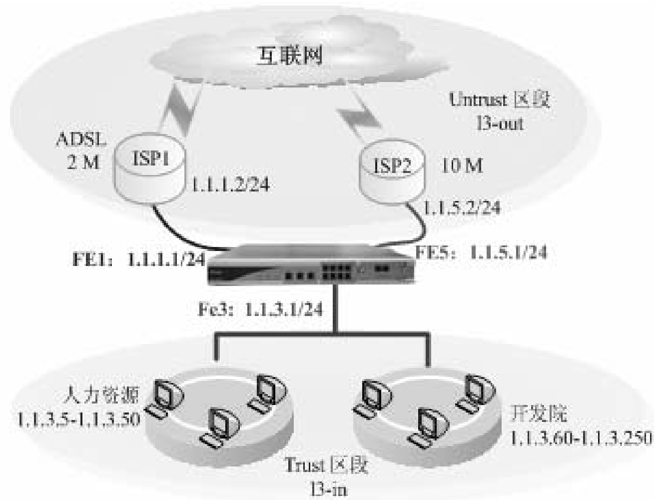
在配置策略路由时，有个“**固定 IP(Fixed IP)**”的选项。当有多条出口实现均衡时，如果选择“**固定 IP(Fixed IP)**”，则同一个源 IP 永远均衡到某条固定的存活的线路，如果不选择“**固定 IP(Fixed IP)**”，同一个源 IP 可能均衡到不同的存活的线路。对于一些端口会发生变化的协议（例如 MSN、FTP），一定要选择“**固定 IP(Fixed IP)**”选项，否则可能出现访问失败。

11.4　CPU 主动路由

当 DPF-Series 设备自身需要和其它设备通信，例如带内网管、记录邮件日志、发送信息到 Aceporter 等，这时需要创建一条 CPU 到目标设备的路由。对于策略路由需要创建一条到目标地址且源安全区是 SELF 的路由。

11.5 范例：策略路由

在如图的示例中， 2M 的 ADSL 线路和 10M 线路分别接在 DPF-Series 设备的 FE1 和 FE5 口上，内网接在 FE3 上。要求在两个 ISP 都正常时，人力资源走 ADSL，开发人员走宽带线路，以实现流量均衡。但当其中一条 ISP 出现故障时，可以方便地切换到另一条 ISP 上，对应用完全透明。



为此我们设定两个 isp 池，isppool-hr 和 isppool-dev，并且定义 ADSL 的 ISP 为 isp-adsl，10M 的 ISP 为 isp-10。isppool-hr 包含成员 isp-adsl（优先级为 2）和 isp-10（优先级为 1），isppool-dev 也包含成员 isp-adsl（优先级为 5）和 isp-10（优先级为 6）。并在策略中指明人力资源的出口为 isppool-hr，开发人员的出口为 isppool-dev。由于 isppool-hr 中 isp-adsl 的优先级高，所以正常情况下人力资源走 ADSL。而 isppool-dev 中 isp-10 的优先级高，正常情况下开发人员走 10M 线路。一旦某个 ISP 出现故障可以切换到优先级低的 ISP，对人力资源和开发的员工来说是完全透明的。

CLI

1. 接口
```
set vif vif1 zone l3-out
set vif vif5 zone l3-out
set vif vif3 zone l3-in
set vif vif1 ip 1.1.1.1 netmask 255.255.255.0
set vif vif3 ip 1.1.3.1 netmask 255.255.255.0
set vif vif5 ip 1.1.5.1 netmask 255.255.255.0
set vif vif1 filters enable web,telnet,ping
set vif vif3 filters enable web,telnet,ping
set vif vif5 filters enable web,telnet,ping
```
2. isp/isppool
```
eum set isp isp-adsl ip 1.1.1.2 dns1 202.96.134.133 dns2 202.96.154.8 track-enable
eum set isp isp-10 ip 1.1.5.2 dns1 202.96.134.133 dns2 202.96.154.8 track-enable
eum set isp-pool isppool-hr
eum set isp-pool isppool-hr isp isp-adsl priority 2 balance 8
eum set isp-pool isppool-hr isp isp-10 priority 1 balance 8
eum set isp-pool isppool-dev
eum set isp-pool isppool-dev isp isp-adsl priority 5 balance 8
eum set isp-pool isppool-dev isp isp-10 priority 6 balance 8
```
3. 策略路由
```
set policy-route src-zone l3-in sip 1.1.3.5-1.1.3.50 stick-sip dip ANY protocol 0 isp-pool isppool-hr
```

set policy-route src-zone l3-in sip 1.1.3.60-1.1.3.250 stick-sip dip ANY protocol 0 isp-pool isppool-dev
set policy-route src-zone SELF sip ANY stick-sip dip ANY protocol 0 isp-pool isppool-hr

4. 策略

firewall set policy from ANY to ANY src-addr ANY dst-addr ANY service ANY action permit status enable

WEB 配置

WEB 的配置 CLI 的配置相对应：

1. 接口

进入 **网络配置(NETWORK)->网络接口(Interfaces)->Virtual**，修改 vif1 和 vif5 关联的 zone 为 l3-out，vif3 关联的 zone 为 l3-in；分别为 vif1、vif3 和 vif5 添加 IP 地址为：1.1.1.1/24、1.1.3.1/24 和 1.1.5.

虚拟接口 新增

序号	名称	物理接口/汇聚口	VLAN	IP地址1/掩码	工作模式	区域	有效	操作
共 9 条记录 当前第 1 页								
1	vif0	lan0	1		透明模式	l2-in	是	
2	vif1	lan1	1		透明模式	l2-in	是	
3	vif2	lan2	1		透明模式	l2-in	是	
4	vif3	lan3	1		透明模式	l2-in	是	
5	vif4	lan4	1		透明模式	l2-in	是	
6	vif5	lan5	1		透明模式	l2-in	是	
7	vif6	lan6	1		透明模式	l2-in	是	
8	vif7	lan7	1		透明模式	l2-in	是	
9	vif9	wan0	1		透明模式	l2-in	是	

图21.接口1

2. ISP/isppool

先要定义 ISP，如果有多个 ISP 就需要分别定义。

进入**系统配置管理(SYSTEM)->Objects->ISPs->新增(Create New)**，填入相应的 IP 和 DNS

新增ISP 提交 取消 返回

名称	isp_ads1		
注释			
类型	⦿ IP ○ PPPoE		
IP地址	1.1.1.2	DNS IP地址1	202.96.134.133
DNS IP地址2	202.96.154.8	DNS IP地址3	0.0.0.0
侦测允许	☑		
侦测目标			

图22.ISP(1)

3. 策略路由

进入 **网络配置(NETWORK)-> 路由配置(Routing)->Policy 路由配置(Routing)->新增(Create New)**，

为人力资源的员工创建策略路由，源 IP 为 1.1.3.5-1.1.3.50，ISP pool 为 isppool-hr；选择“**固定 IP(Fixed IP)**”

新增策略路由		提交 取消 返回	
位置	○ 置顶 ○ 在 之前 ⊙ 最后		
源安全区	l3-in	固定ISP	☑
源组			
源地址	1.1.3.5-1.1.3.50		
目的地址			
协议		目的端口	-
ISP或ISP池	○ ISP ⊙ ISP池	isppool-hr	

图23. 策略路由(1)

为开发的员工创建策略路由，源 IP 为 1.1.3.60－1.1.3.250，ISP pool 为 isppool-dev；选择“**固定 IP(Fixed IP)**”

新增策略路由		提交 取消 返回	
位置	○ 置顶 ○ 在 之前 ⊙ 最后		
源安全区	l3-in	固定ISP	☑
源组			
源地址	1.1.3.60－1.1.3.250		
目的地址			
协议		目的端口	-
ISP或ISP池	○ ISP ⊙ ISP池	isppool-dev	

图24.策略路由(2)

再建立一条从 SELF 区域（CPU）到外网的路由，这条路由用于 DPF-Series 设备主动访问外网；选择“**固定 IP(Fixed IP)**”

新增策略路由		提交 取消 返回	
位置	○ 置顶 ○ 在 之前 ⊙ 最后		
源安全区	SELF	固定ISP	☑
源组			
源地址			
目的地址			
协议		目的端口	-
ISP或ISP池	○ ISP ⊙ ISP池	isppool-dev	

图25.策略路由(3)

11.6 路由的合理均衡

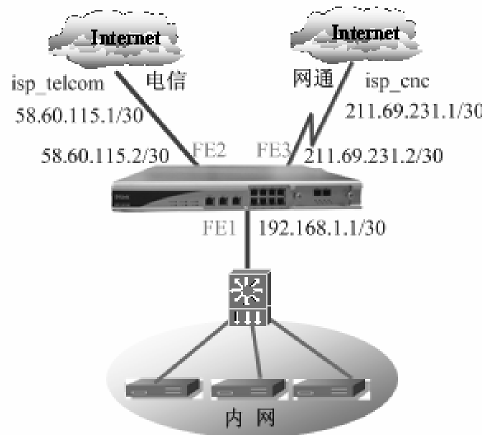
当有多条 ISP 时，DPF-Series 设备支持路由最佳选择和均衡。比如一个企业有两条 ISP：网通和电信。DPF-Series 设备在选路时，如果发现目标是到电信的地址，就让其走电信线路；如果目标是到网通的地址，就让其走网通线路。其它地址就利用策略路由在电信和网通线路之间随机均衡。

对于多条 ISP 链路的网络，我们收集了电信、网通、铁通和联通等运营商的地址段，用高级型静态路由包含各运营商的目标地址段，下一跳指向其对应的 ISP，并且把这些路由制作成一个脚本，然后只需要把这个脚本导入 DPF-Series 设备即可。最后再配置策略路由，将出口指向 ISP POOL，这个 POOL 中包含所有的 ISP。这样就可以实现，到运营商地址段的报文匹配高级型静态路由，通过其对应的 ISP 到达互联网；剩下的就匹配策略路由，在各个 ISP 之间均衡。并且其中一条 ISP 出现故障时，可以方便地切换到另一条 ISP 上，对应用完全透明。

11.7 范例：综合路由

在本例中，一条电信线路和一条网通线路分别接在 DPF-Series 设备的 FE2 和 FE3 口上，内网接在 FE1 上。当两条链路都正常时，要求内网访问互联网时，如果目的是到电信的地址段，则通过电信线路出去，如果目的是到网通的地址段，则通过网通线路出去；其它目的地址段在两条线路之间随机均

衡；并且要求其中一条 ISP 出现故障时，可以方便地切换到另一条 ISP 上，对应用完全透明。



为此我们设定两个 isp，isp_telcom 和 isp_cnc，分别对应电信和网通的的 ISP；然后再定义一个 ISP 池（telcom_cnc)包含成员 isp_telcom 和 isp_cnc，优先级都为 2。然后用脚本导入高级静态路由，再在策略路由中内网访问互联网的出口为 telcom_cnc。由于高级型静态路由的优先级高于策略路由，且 ISP 池(telcom_cnc)中两个 ISP 的优先级相同，所以两条链路都正常时，目的是到电信的地址段，就通过电信线路出去，如果目的是到网通的地址段，就走网通线路出去；其它目的地址段在两条线路之间随机均衡；并且其中一条 ISP 出现故障时，可以方便地切换到另一条 ISP 上，对应用完全透明。

CLI

1. 接口

```
set vif vif1 zone l3-in
set vif vif2 zone l3-out
set vif vif3 zone l3-out
set vif vif1 ip 192.168.1.1 netmask 255.255.255.0
set vif vif2 ip 58.60.115.2 netmask 255.255.255.252
set vif vif3 ip 211.69.231.2 netmask 255.255.255.252
set vif vif2 nat
set vif vif3 nat
set vif vif1 filters enable web,telnet,ping
set vif vif3 filters enable web,telnet,ping
set vif vif5 filters enable web,telnet,ping
```

2. isp/isppool

```
eum set isp isp_telcom type ip ip 58.60.115.2 dns1 202.96.134.133 dns2 202.96.154.8 track-enable
eum set isp isp_cnc type ip ip 211.69.231.2 dns1 202.96.134.133 dns2 202.96.154.8 track-enable
eum set isp-pool telcom_cnc
eum set isp-pool telcom_cnc isp isp_telcom priority 2 balance 5
eum set isp-pool telcom_cnc isp_cnc priority 2 balance 3
```

3. 静态路由

由于篇幅有限，这里只截取两条作为代表，完整的路由请参考 Dlink 公司提供的脚本

```
set route ip 58.16.0.0 255.255.0.0 isp_cnc
set route ip 58.32.0.0 255.248.0.0 isp_telcom
```

4. 策略路由

```
set policy-route src-zone l3-in sip ANY stick-sip dip ANY protocol 0 isp-pool telcom_cnc
set policy-route src-zone SELF sip ANY stick-sip dip ANY protocol 0 isp-pool telcom_cnc
```

5. 策略

```
firewall set policy from ANY to ANY src-addr ANY dst-addr ANY service ANY action permit
```

status enable

WEB 配置

WEB 的配置 CLI 的配置相对应：

1. 接口

   进入 **网络配置(NETWORK)->网络接口(Interfaces)->Virtual**，修改 vif2 和 vif3 关联的 zone 为 l3-out，vif1 关联的 zone 为 l3-in；分别为 vif1、vif2 和 vif3 添加 IP 地址为：192.168.1.1/24、58.60.115.2/30 和 211.69.231.2/30

虚拟接口 新增

序号	名称	物理接口/汇聚口	VLAN	IP地址1/掩码	工作模式	区域	有效	操作
共 9 条记录 当前第 1 页								
1	vif0	lan0	1		透明模式	l2-in	是	
2	vif1	lan1	1		透明模式	l2-in	是	
3	vif2	lan2	1		路由模式	l3-out	否	
4	vif3	lan3	1		路由模式	l3-out	否	
5	vif4	lan4	1		透明模式	l2-in	是	
6	vif5	lan5	1		透明模式	l2-in	是	
7	vif6	lan6	1		透明模式	l2-in	是	
8	vif7	lan7	1		透明模式	l2-in	是	
9	vif9	wan0	1		透明模式	l2-in	是	

图26.vif

2. ISP/isppool

   先要定义 ISP，如果有多个 ISP 就需要分别定义。

   进入**系统配置管理(SYSTEM)->Objects->ISPs->新增(Create New)**，填入相应的 IP 和 DNS 参数

ISP 新增

序号	名称	IP地址	DNS1	DNS2	DNS3	有效	操作
共 2 条记录							
1	isp-cnc	211.69.231.2	202.96.128.86	0.0.0.0	0.0.0.0		
2	isp-telcom	58.60.115.2	202.96.128.86	0.0.0.0	0.0.0.0		

图27.isp(1)

然后再建立一个 ISP pool：telcom_cnc

新增ISP池 提交 取消 返回

名称	telcom-cnc
物理隔离	⦿ 启用 ○ 禁用

图28.isp pool

建立好 ISP pool 后，点击“**member**”，添加 ISP 成员，并赋予优先级。这里由于要实现链路均衡，所以两个 isp 的优先级相等，各自分担的 Balance 为 5 和 3。同一个优先级的 banlace 总和必须为 8，每个 ISP 分担的 balance 根据链路的带宽来定，带宽大的可以多分担一些。

ISP池 新增

序号	名称	ISP数量	物理隔离	操作
共 1 条记录				
1	telcom-cnc	0	启用	

图29.isp pool

3. 静态路由

   由于篇幅有限，这里只列举了两条作为代表，完整的路由请参考 Dlink 公司提供的脚本

   进入 **网络配置(NETWORK)->路由配置(Routing)->网络路由(Static Routing)->新增(Create New)**，添加一条到网通地址段的路由，下一跳(gateway/ISP)配置为 isp_cnc：

新增网络路由表			提交 取消 返回
IP地址	58.16.0.0	子网掩码	255.255.0.0
网关/ISP	isp_cnc		
*IP地址 0.0.0.0 掩码 0.0.0.0 代表缺省路由			

图30. static routing

再添加一条到电信地址段的路由，下一跳(gateway/ISP)配置为 isp_telcom：

新增网络路由表			提交 取消 返回
IP地址	58.32.0.0	子网掩码	255.248.0.0
网关/ISP	isp-telcom		
*IP地址 0.0.0.0 掩码 0.0.0.0 代表缺省路由			

图31.static routing

4. 策略路由

进入 **网络配置(NETWORK)-> 路由配置(Routing)->Policy 路由配置(Routing)->新增(Create New)**，

为内网创一条建策略路由，源 zone 选择为 l3-in，ISP pool 为 telcom_cnc；选择“**固定 IP(Fixed IP)**”

新增策略路由			提交 取消 返回
位置	⦿ 置顶 ○ 在 ______ 之前 ○ 最后		
源安全区	l3-in	固定ISP	☑
源组	ANY		
源地址	ANY		
目的地址	ANY		
协议	ANY	目的端口	-
ISP或ISP池	○ ISP ⦿ ISP池	telcom_cnc	

图32. 策略路由(1)

再建立一条从 SELF 区域（CPU）到外网的路由，用于 DPF-Series 设备主动访问外网；选择“**固定 IP(Fixed IP)**”

新增策略路由			提交 取消 返回
位置	○ 置顶 ○ 在 ______ 之前 ⦿ 最后		
源安全区	SELF	固定ISP	☑
源组	ANY		
源地址	ANY		
目的地址	ANY		
协议	ANY	目的端口	-
ISP或ISP池	○ ISP ⦿ ISP池	telcom_cnc	

图33.策略路由(2)

5. 策略

进入 **安全(SECURITY)-> 安全策略(Policies)->新增(Create New)**，添加一条全局的 permit all 的策略

策略列表: All

新增 | 全选 提交 | 清

序号	源地址/用户/地址簿	目的地址/用户/地址簿	定时计划	安全配置	服务	匹配计数	动作	状态	操作
▼ 全局 共 1 条记录									清
1	ANY	ANY			ANY	0	permit	☑	

图34.策略

12 安全策略

12.1 简介

安全策略用来控制通过 DPF-Series 设备的所有 IP 数据流(非 IP 数据流不受安全策略的控制)，整个安全策略分成 **匹配条件**、**匹配后执行的动作** 和 **高级行为** 三个部分。

匹配条件 包含以下几种，这些条件可以任意组合成为策略的匹配条件

- 源安全区域： 数据流来自哪个安全区
- 目的安全区域： 数据流将去往哪个安全区
- 源用户组： 数据流对应的源认证用户所在的用户组
- 目的用户组： 数据流对应的目的认证用户所在的用户组
- 源 IP 地址范围： 数据流的源 IP 地址(或者地址段)
- 目的 IP 地址范围： 数据流的目的 IP 地址(或者地址段)
- 源用户名： 数据流对应的源认证用户的用户名
- 目的用户名： 数据流对应的目的认证用户的用户名
- 服务类型： 数据流的协议类型，比如 HTTP、FTP 等协议
- 时间段(Schedule)： 可以分时段控制数据流，比如 9：00～12：00 和 14：00～18：00 这段上班时间，不允许员工用 QQ。

匹配后执行的 **动作** 包括：

- PERMIT：表示允许报文通过。
- DENY：表示拒绝报文通过。
- REJECT：也表示拒绝报文通过，与 deny 不同的是，除了丢弃此包外，还会给报文的发送者回复一个 icmp 不可达报文。
- PAT：表示符合策略的报文要作 PAT 转换。
- AUTH：表示符合策略的报文需要认证。
- TUNNEL：表示符合策略的报文执行 IPSec VPN 处理。

安全策略的 **高级行为** 包括：

- 安全控制(Security Config)：对数据量进行安全控制，包括对 IM/P2P、内容过滤、IPS 的控制
- 流量控制(QoS)：对数据量的带宽进行限制，比如说某个用户对 P2P 的访问只有 100K 的带宽。

安全策略的 **类型**:

- 区域间的安全策略：指定了源安全区域(源安全区不是 ANY)和目的安全区域(目的安全区不是 ANY)的安全策略。
- 全局安全策略：没有指定源安全区域(源安全区是 ANY)或者目的安全区域(目的安全区是 ANY)的安全策略。全局的安全策略优先级低于区域间的安全策略。
- 缺省安全策略：系统缺省设置了一条安全策略，就是 ANY to ANY 的拒绝策略(即缺省情况下所有报文都会被丢弃)，这条策略没有显示在界面上。

安全策略的 **优先级**:

DPF-Series 设备在根据一个 IP 报文的匹配条件查找安全策略表时，首先进行区域间的策略查找，找到第一个匹配的策略则停止查找。否则再查找全局安全策略，找到第一个匹配则停止查找。如果全局策略也没有查到，则应用缺省的安全策略。同一类安全策略，ID 号小的优先级高。例如，在 “l3-in --> l3-out”的策略中，ID 为 1 的策略是允许 Trust 区段（l3-in）的主机 A 访问 Untrust 区段（l3-out）的服

务器 B 的 HTTP 请求，ID 为 2 的策略是拒绝主机 A 访问服务器 B 的 HTTP 请求。则当 DPF-Series 设备接收到从主机 A 到服务器 B 的 HTTP 请求时，匹配到 ID 为 1 的策略后，不再查找下一条策略，所以 DPF-Series 设备将允许此报文通过。

缺省情况下，最新创建的策略出现在同一类安全策略组列表的底部。新建时有一个选项允许将策略定位在列表的顶部。也可以根据需要将策略移动到列表中的不同位置。创建策略后，始终都可以返回到该策略进行修改。除修改和重新排序策略外，还可以删除策略。

安全策略中的 **地址薄:**

DPF-Series 设备还支持定义地址薄的方式把将具有相同策略的零散的 IP 地址(或者地址段)汇聚到一起，可以简化策略的配置。比如，将“192.168.5.1、212.59.6.89、212.59.6.95、49.50.58.6、58.231.1.1/28”这几个地址(或者地址段)定义为一个地址簿，然后在配置策略时引用地址簿的名称。这样就只需要定义一条策略，从而简化了策略的配置。

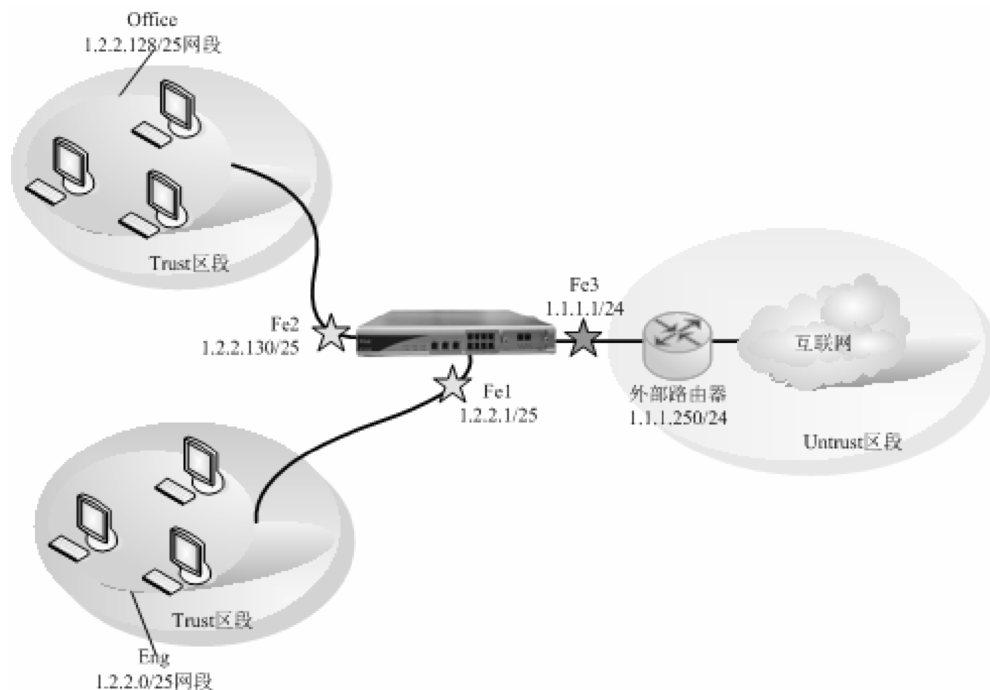
12.2 范例一

一个小的软件公司已将其内部网络分成两个子网，这两个子网都分别在两个 Trust 区段中。这两个区段为：

- 工程 (定义为“Eng”，对应 IP 1.2.2.0/25)
- 公司的其余部分 (定义为“Office”，对应 IP 1.2.2.128/25)。

下面介绍了对以下用户的一组典型策略:

- Eng：经理可使用所有的服务；其他成员除 FTP 和 POP3 外，可使用用于出站信息流的所有服务。这里给经理预留五个 IP（1.2.2.2-1.2.2.6）。
- Office：可以访问外网。



CLI

1. 区段

   set zone new eng router trust in-vr
   set zone new office router trust in-vr

2. 接口

   set vif vif1 zone eng
   set vif vif2 zone office
   set vif vif3 zone l3-out
   set vif vif1 ip 1.2.2.1 netmask 255.255.255.128
   set vif vif2 ip 1.2.2.130 netmask 255.255.255.128
   set vif vif3 ip 1.1.1.1 netmask 255.255.255.0
   set vif vif1 filters enable web,telnet,ping
   set vif vif2 filters enable web,telnet,ping
   set vif vif3 filters enable web,telnet,ping

3. 路由

   set route ip 0.0.0.0 0.0.0.0 1.1.1.250

4. 策略

   firewall set policy from eng to l3-out src-addr 1.2.2.7-1.2.2.126 dst-addr ANY service FTP action deny status enable
   firewall set policy from eng to l3-out src-addr 1.2.2.7-1.2.2.126 dst-addr ANY service POP3 action deny status enable
   firewall set policy from eng to l3-out src-addr ANY dst-addr ANY service ANY action permit status enable
   firewall set policy from office to l3-out src-addr ANY dst-addr ANY service ANY action permit status enable

WEB 配置

WEB 的配置与 CLI 的配置相对应：

1. 区段

   进入 **网络配置(NETWORK)->安全区域(Zones)->新增(Create New)**，添加两个路由模式的区段，名为 eng 和 office 属于信任域

新增安全区域			提交 取消 返回
名称	eng		
模式	路由模式	信任	信任

图35.　区段配置

新增安全区域			提交 取消 返回
名称	office		
模式	路由模式	信任	信任

图36.　区段配置

2. 接口

   进入 **网络配置(NETWORK)->网络接口(Interfaces)->Virtual**，修改 vif1 的 zone 为 eng，然后再点击 “**Set VIF IP**”按钮，添加 IP 1.2.2.1/25, 并允许web ,telnet, ping服务。

修改虚拟接口					提交 取消 返回
虚接口名称	vif1	物理口/汇聚接口	lan1	有效	⦿ 是 ○ 否
VLAN	1	区域	eng		
加VLAN标签	☐	工作模式	透明模式		
报文允许	☑ web ☑ telnet ☐ ssh ☑ ping ☐ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

图37. 接口

同理配置 vif2 和 vif3 ，分别对应 zone 为 office 和 l3-out，IP 分别设置为1.2.2.130/25 和 1.1.1.1/24。在虚拟接口的全局模式下，可以看到刚才配置的三个接口的 IP 和相关信息，如图：

虚拟接口 新增

序号	名称	物理接口/汇聚口	VLAN	IP地址1/掩码	工作模式	区域	有效	操作
共 9 条记录 当前第 1 页								
1	vif0	lan0	1		透明模式	l2-in	是	
2	vif1	lan1	1		透明模式	l2-in	是	
3	vif2	lan2	1		路由模式	office	否	
4	vif3	lan3	1		路由模式	l3-out	否	
5	vif4	lan4	1		透明模式	l2-in	是	
6	vif5	lan5	1		透明模式	l2-in	是	
7	vif6	lan6	1		透明模式	l2-in	是	
8	vif7	lan7	1		透明模式	l2-in	是	
9	vif9	wan0	1		透明模式	l2-in	是	

图38. 接口

3. 路由

进入 **网络配置(NETWORK)->路由配置(Routing)->网络路由(Static Routing)->新增(Create New)**，添加一条到 1.1.1.250 的默认路由：

新增网络路由表 提交 取消 返回

IP地址	0.0.0.0	子网掩码	0.0.0.0
网关/ISP	1.1.1.250		
*IP地址 0.0.0.0 掩码 0.0.0.0 代表缺省路由			

图39. 路由

4. 策略

进入 **安全(SECURITY)->安全策略(Policies)->新增(Create New)**，源安全区选择 eng，目的安全区选择 l3-out，动作选择 deny，源地址为 1.2.2.7-1.2.2.126，目的地址为 ANY ，服务选择 FTP

新增安全策略 提交 取消 返回

位置	○ 置顶 ○ 在 ____ 之前 ⊙ 最后		
安全区			
源安全区	eng	目的安全区	ANY
地址/用户/地址簿			
	⊙ 源 地址 ○ 用户 ○ 地址簿	1.2.2.7-1.2.2.126	
	⊙ 目的地址 ○ 用户 ○ 地址簿	ANY	
动作	DENY	服务	FTP
日志	☐ log		
防病毒	☐ 防病毒		
使能	⊙ 启用 ○ 禁用	☐ 显示高级	

图40. 策略

进入 **安全(SECURITY) ->安全策略(Policies)->新增(Create New)**，源安全区选择 eng，目的安全区选择 l3-out， 动作选择 deny，源地址为 1.2.2.7-1.2.2.126，目的地址为 ANY，服务选择 POP3

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 之前 ⦿ 最后		
安全区			
源安全区	ANY	目的安全区	ANY
地址/用户/地址簿			
	⦿ 源 地址 ○ 用户 ○ 地址簿	1.2.2.7-1.2.2.126	
	⦿ 目的地址 ○ 用户 ○ 地址簿	ANY	
动作	DENY	服务	POP3
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☐ 显示高级	

图41. 策略

进入 **安全(SECURITY)->安全策略(Policies)->新增(Create New)**, 源安全区为 eng，目的安全区为 l3-out， permit any

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 之前 ⦿ 最后		
安全区			
源安全区	eng	目的安全区	l3-out
地址/用户/地址簿			
	⦿ 源 地址 ○ 用户 ○ 地址簿	ANY	
	⦿ 目的地址 ○ 用户 ○ 地址簿	ANY	
动作	PERMIT	服务	ANY
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☐ 显示高级	

图42. 策略

进入 **安全(SECURITY)->安全策略(Policies)->新增(Create New)**，创建源安全区为 office，目的安全区为 l3-out，permit any

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 之前 ⦿ 最后		
安全区			
源安全区	office	目的安全区	l3-out
地址/用户/地址簿			
	⦿ 源 地址 ○ 用户 ○ 地址簿	ANY	
	⦿ 目的地址 ○ 用户 ○ 地址簿	ANY	
动作	PERMIT	服务	ANY
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☐ 显示高级	

图43. 策略

最后，在 policy list 里选择 all 就可以看到刚才添加的策略：

策略列表: All

新增 ☐ 全选 提交

序号	源地址/用户/地址簿	目的地址/用户/地址簿	定时计划	安全配置	服务	匹配计数	动作	状态	操作
▼ eng -> l3-out 共 1 条记录									清
1	ANY	ANY			ANY	0	permit	☑	
▼ office -> l3-out 共 1 条记录									清
1	ANY	ANY			ANY	0	permit	☑	
▼ 全局 共 2 条记录									清
1	ANY	ANY			ANY	0	permit	☑	
2	1.2.2.7-1.2.2.126	ANY			FTP	0	deny	☑	

图44. 策略

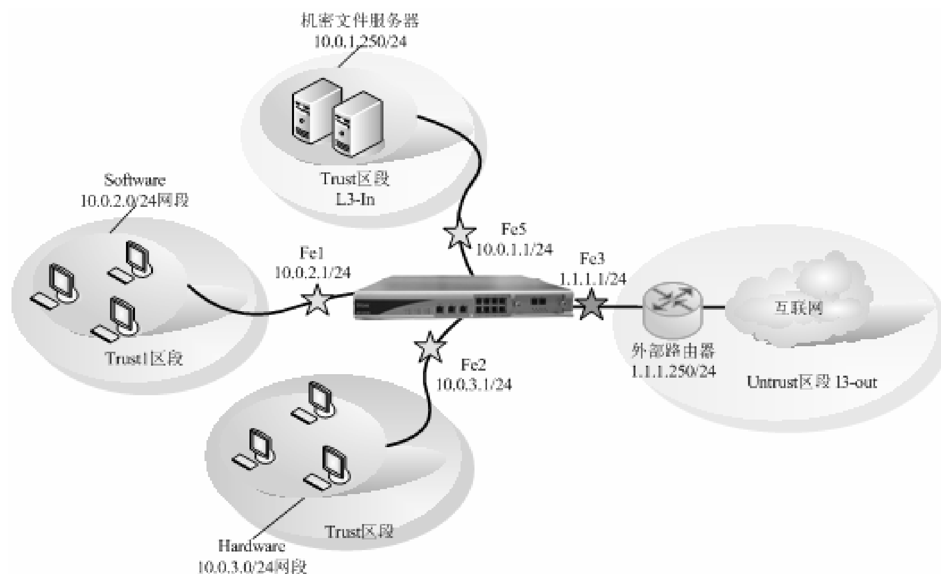
12.3 范例二

某公司的开发院有软件部门和硬件部门，都位于 Trust 区段中。这两个区段为：

- 软件（ 定义为“software”，对应 IP 10.0.2.0/24)
- 硬件（ 定义为“hardware”，对应 IP 10.0.3.0/24)

要求实现以下策略:

- 软件部和硬件部之间不需要认证就可以相互访问
- 软件部和硬件部访问互连网时需要认证
- 软件部和硬件部访问互连网时需要做 PAT 转换
- 开发院有一台存放机密文件的服务器，只能是软件部和硬件部的经理才可以访问



定义 soft_grp 和 hard_grp 两个用户组。分别将软件部和硬件部的员工的用户名绑定到这两个组里去。软件部经理的 IP 为 10.0.2.251/24，硬件部经理的 IP 为 10.0.3.241/24。机密文件服务器的 IP 为 10.0.1.250。这里省去了认证用户的设置。

CLI

1. 区段

```
set zone new software router trust in-vr
set zone new hardware router trust in-vr
```

2. 接口

```
set vif vif1 zone software
set vif vif2 zone hardware
set vif vif5 zone l3-in
set vif vif3 zone l3-out
set vif vif1 ip 10.0.2.1 netmask 255.255.255.0
set vif vif2 ip 10.0.3.1 netmask 255.255.255.0
set vif vif3 ip 1.1.1.1 netmask 255.255.255.0
set vif vif5 ip 10.0.1.1 netmask 255.255.255.0
set vif vif1 filters enable web,telnet,ping
set vif vif2 filters enable web,telnet,ping
set vif vif3 filters enable web,telnet,ping
set vif vif5 filters enable web,telnet,ping
```

3. 路由

set route ip 0.0.0.0 0.0.0.0 1.1.1.250

4. 用户组

eum set group soft_grp authentication web_8021x authorization normal accounting noaccounting
eum set group hard_grp authentication web_8021x authorization normal accounting noaccounting

5. pat pool

firewall set pat-pool dev_pool 1.1.1.2 1.1.1.3

6. 地址薄

firewall set address-book dev_book address 10.0.3.241
firewall set address-book dev_book item 2 address 10.0.2.251

7. 策略

firewall set policy from hardware to software src-addr ANY dst-addr ANY service ANY action permit status enable
firewall set policy from software to hardware src-addr ANY dst-addr ANY service ANY action permit status enable
firewall set policy from ANY to ANY src-addr-book dev_book dst-addr 10.0.1.250 service ANY action permit status enable
firewall set policy from software to l3-out src-addr ANY dst-addr ANY service DNS action pat pat-pool dev_pool pat-fix-port status enable
firewall set policy from hardware to l3-out src-addr ANY dst-addr ANY service DNS action pat pat-pool dev_pool pat-fix-port status enable
firewall set policy from software to l3-out src-addr ANY dst-addr ANY service ANY action auth auth-server-type default status enable
firewall set policy from hardware to l3-out src-addr ANY dst-addr ANY service ANY action auth auth-server-type default status enable
firewall set policy from software to l3-out src-addr ANY src-group soft_grp dst-addr ANY service ANY action pat pat-pool dev_pool pat-fix-port status enable
firewall set policy from hardware to l3-out src-addr ANY src-group hard_grp dst-addr ANY service ANY action pat pat-pool dev_pool pat-fix-port status enable

WEB 配置

WEB 配置与 CLI 的配置相对应：

1. 区段

进入 **网络配置(NETWORK)->安全区域(Zones)->新增(Create New)**，添加两个名为 software 和 hardware 的路由模式的区段，属于trust区域。建立好后，可以在区段的全局模式下，看到刚才创建的两个区段，如下图：

安全区域 新增

序号	名称	信任	模式	操作
共 9 条记录				
3	l3-in	信任	路由模式	
4	l3-out	不信任	路由模式	
5	l2-in	信任	透明模式	
6	l2-out	不信任	透明模式	
7	eng	信任	路由模式	
8	office	信任	路由模式	
126	BCAST	不信任	N/A	
127	SELF	不信任	N/A	
128	NULL	不信任	N/A	

图45. 区段配置

2. 接口

进入 **网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)-> vif1**，修改 zone 为 software，然后再点击 “**Set VIF IP**”按钮, 添加 IP 10.0.2.1/24, 并允许web ,telnet, ping服务。

修改虚拟接口					提交 取消 返回
虚接口名称	vif1	物理口/汇聚接口	lan1	有效	○ 是 ⊙ 否
VLAN	1	区域	software		
加VLAN标签	☐	工作模式	透明模式		
报文允许	☑ web ☑ telnet ☐ ssh ☑ ping ☐ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

图46. 接口

同理配置 vif2 、vif3 和 vif5，分别对应 zone 为 hardware、l3-in 和 l3-out，IP 分别设置为 10.0.3.1/24、1.1.1.1/24 和 10.0.1.1/24。接口配置完成后，可以在虚拟接口的全局模式下看到刚才配置的四个接口的 IP 和相关信息， 如下图所示：

虚拟接口 新增

共 9 条记录 当前第 1 页

序号	名称	物理接口/汇聚口	VLAN	IP地址1/掩码	工作模式	区域	有效	操作
1	vif0	lan0	1		透明模式	l2-in	是	
2	vif1	lan1	1		透明模式	l2-in	是	
3	vif2	lan2	1		路由模式	office	否	
4	vif3	lan3	1		路由模式	l3-out	否	
5	vif4	lan4	1		透明模式	l2-in	是	
6	vif5	lan5	1		透明模式	l2-in	是	
7	vif6	lan6	1		透明模式	l2-in	是	
8	vif7	lan7	1		透明模式	l2-in	是	
9	vif9	wan0	1		透明模式	l2-in	是	

图47. 查看接口

3. 路由

进入 **网络配置(NETWORK)->路由配置(Routing)->网络路由(Static Routing)->新增(Create New)**，添加一条到 1.1.1.250 默认的路由

新增网络路由表			提交 取消 返回
IP地址	0.0.0.0	子网掩码	0.0.0.0
网关/ISP	1.1.1.250		
*IP地址 0.0.0.0 掩码 0.0.0.0 代表缺省路由			

图48. 路由

4. 用户组

进入 **USER->User Group->新增(Create New)**，创建两个用户组 soft_grp 和 hard_grp，认证策略和授权策略都调用系统默认参数

新增认证用户		提交 取消 返回
名称	soft_grp	
注释		
组	normal_group	☐ 显示高级

图49. 用户组

建立完成后，可以看到刚才创建的两个用户组：

认证用户信息 新增 清除

序号	名称	组	IP地址	MAC地址	VLAN	端口号	黑名单控制	操作
共 0 条记录 当前第 1 页								
1	hard_grp	normal_group	0.0.0.0	00-00-00-00-00-00			启用	
2	soft_grp	normal_group	0.0.0.0	00-00-00-00-00-00			启用	

图50. 用户组

5. Pat pool

进入 **安全(SECURITY)-> NAT ->Ip Pool->新增(Create New)**, 创建一个名为 dev_pool 的 PAT 池。

新增端口转换地址池 提交 取消 返回

名称	dev_pool		
注释			
起始转换IP	1.1.1.2	结束转换IP	1.1.1.3

图51. Pat pool

6. 地址薄

进入 **安全(SECURITY)-> 安全策略(Policies)->Address Book->新增(Create New)**，创建一个名为 dev_book 的地址薄，包含两个部门经理的 IP：10.0.3.241 和 10.0.2.251

新增地址 提交 取消 返回

名称	dev_book
注释	
添加第一个成员：	
地址	10.0.3.241 10.0.2.251

图52. 地址薄

7. 策略

进入 **安全(SECURITY)->安全策略(Policies)->新增(Create New)**，添加策略。完成后，在 policy list 里选择 all 就可以看到刚才添加的策略

策略列表: All

新增 □全选 提交

序号	源地址/用户/地址簿	目的地址/用户/地址簿	定时计划	安全配置	服务	匹配计数	动作	状态	操作
eng -> l3-out 共 1 条记录									
1	ANY	ANY			ANY	0	permit	☑	
office -> l3-out 共 1 条记录									
1	ANY	ANY			ANY	0	permit	☑	
全局 共 2 条记录									
1	ANY	ANY			ANY	0	permit	☑	
2	1.2.2.7-1.2.2.126	ANY			FTP	0	deny	☑	

图53. 策略

12.4 范例三：疑难排除

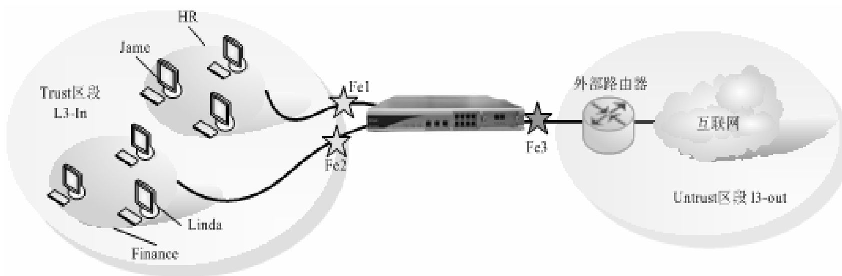
某公司的财务部和人力资源两个部门都位于 Trust 区段 (l3-in)。定义这两个部门为：

◆ finance

◆ HR

要求实现以下策略：

◆ 两个部门的普通员工之间不能相互访问
◆ 两个部门的经理可以相互访问
◆ 两个部门的所有员工访问互连网时需要认证



定义 hr_grp 和 fin_grp 两个用户组。分别将人力资源和财务部的员工的用户名绑定到这两个组里去。为人力资源部的经理配置一个用户名 Jame，为财务部的经理配置一个用户名 Linda。为简单起见，这里省去其它的配置，只列举了安全策略的配置。

CLI

firewall set policy from l3-in to l3-out src-addr ANY dst-addr ANY service ANY action auth auth-server-type default status enable
firewall set policy from l3-in to l3-out src-addr ANY dst-addr ANY service ANY action permit status enable firewall set policy from ANY to ANY src-user Jame dst-user Linda service ANY action permit status enable

WEB

策略列表: All

新增 ☐ 全选 提交

序号	源地址/用户/地址簿	目的地址/用户/地址簿	定时计划	安全配置	服务	匹配计数	动作	状态	操作
eng -> l3-out 共 1 条记录									
1	ANY	ANY			ANY	0	permit	☑	
office -> l3-out 共 1 条记录									
1	ANY	ANY			ANY	0	permit	☑	
全局 共 2 条记录									
1	ANY	ANY			ANY	0	permit	☑	
2	1.2.2.7-1.2.2.126	ANY			FTP	0	deny	☑	

作了上述配置后发现两个问题：

◆ 人力资源部经理 Jame 可以访问财务部经理 Linda，但是 Linda 不能访问 Jame。
◆ 两个部门的所有员工访问互联网时，无法弹出认证窗口

经检查发现上述配置存在两个错误：

◆ 没有配置财务部经理 Linda 到人力资源部经理 Jame 的策略，因为策略是有方向的，所以 Linda 不能访问 Jame。
◆ 没有配置允许两个部门的员工访问 DNS 服务的策略，所以阻止了认证窗口的弹出

以下就是正确的配置：

CLI

firewall set policy from l3-in to l3-out src-addr ANY dst-addr ANY service DNS action permit status enable
firewall set policy from l3-in to l3-out src-addr ANY dst-addr ANY service ANY action auth auth-server-type default status enable
firewall set policy from l3-in to l3-out src-addr ANY dst-addr ANY service ANY action permit status enable firewall set policy from ANY to ANY src-user Jame dst-user Linda service ANY action permit status enable
firewall set policy from ANY to ANY src-user Linda dst-user Jame service ANY action permit status enable

WEB

策略列表: All

新增 □ 全选 提交 清空

序号	源地址/用户/地址簿	目的地址/用户/地址簿	定时计划	安全配置	服务	匹配计数	动作	状态	操作
▼ eng -> l3-out 共 1 条记录									清除
1	ANY	ANY			ANY	0	permit	☑	
▼ office -> l3-out 共 1 条记录									清除
1	ANY	ANY			ANY	0	permit	☑	
▼ 全局 共 2 条记录									清除
1	ANY	ANY			ANY	0	permit	☑	
2	1.2.2.7-1.2.2.126	ANY			FTP	0	deny	☑	

12.5 Q&A

1. 采用地址簿和采用直接 IP 地址输入有什么区别?

在配置一个安全策略时，直接输入的 IP 地址可以是一个 IP 地址、一个 IP 子网地址或者一段连续的 IP 地址范围; 如: 1.1.1.1、1.1.1.1/24 或者 1.1.1.1-1.1.1.100。而如果希望输入的几个 IP 地址组合是跳跃的 (非连续)时,采用地址薄就比较方便。 如定义一个地址薄包含以下 5 个 IP 地址: 1.1.1.1, 1.1.1.13, 1.1.1.17, 2.2.2.3, 2.2.11.12, 3.3.3.123。

2. 采用用户组和用户名的条件输入有什么特点?

配置一个安全策略时，DPF-Series 设备支持直接输入源/目的用户组或者源/目的用户名作为匹配条件。 这两种条件都是必须和用户认证功能联系到一起，只有在先定义了用户组和用户名的情况下，才可以允许配置这些基于存在的用户组和用户名的策略匹配条件。另外，登陆的用户必须符合这些用户组和用户名时，其发送的 IP 报文才有可能匹配这些安全策略。

如：我们配置一个名为 Mike 的用户不允许使用 HTTP 服务。

CLI 命令为：
firewall set policy from ANY to ANY src-user **Mike** service **HTTP** action deny status enable

WEB 命令为：

策略列表: All

新增 □ 全选 提交 清空

序号	源地址/用户/地址簿	目的地址/用户/地址簿	定时计划	安全配置	服务	匹配计数	动作	状态	操作
▼ 全局 共 1 条记录									清除
1	ANY	ANY			ANY	0	permit	☑	

首先名为 **Mike** 的用户必须在用户认证功能中已经定义，才可以配置这个安全策略。那么什么

时候这个策略起作用呢？只有当用户名为 **Mike** 的主机登陆后，该主机才有可能匹配该安全策略（ 注意：这里说的是主机名，不是 IP 地址。因为用 **Mike** 这个用户名登陆的主机可能是任意的 IP 地址)。

3. Reject 和 Deny 两种执行动作的区别?

Deny 表示 DPF-Series 设备系统自动丢弃相应匹配策略的 IP 报文, 而 Reject 则是在丢弃这个 IP 报文的同时，发送一个错误报文给发送者。从而可以有效防止一些特殊的防火墙探测软件和企图穿越/攻击防火墙的试探报文。

4. 关于到 SELF 安全区域的安全策略和虚拟接口上的报文允许开关的优先级是什么样的?

SELF 安全区域是指 DPF-Series 设备本身，当定义的目的安全区域是 SELF 时，可以控制那些发向 DPF-Series 设备本身的 IP 报文行为。同时在每个虚拟接口上也有一些特殊报文允许开关，如下图所示：

修改虚拟接口 提交 取消 返回

虚接口名称	vif0	物理口/汇聚接口	lan0	有效	◉ 是 ○ 否
VLAN	1	区域	l2-in		
加VLAN标签	☐	工作模式	透明模式		
报文允许	☑ web ☑ telnet ☐ ssh ☑ ping ☐ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

如果这两种策略配置有冲突时，虚拟接口上的配置优先级高。例如：如果在虚拟接口 vif1 上配置了 HTTP 允许，又在安全策略中配置了到 SELF 区段的 HTTP 禁止。因为虚拟接口的配置优先级高，所以从 vif1 收到的 HTTP 报文可以到达 DPF-Series 设备，而从其他虚拟接口收到的 HTTP 报文会被丢弃。

5. 安全策略中的 PAT 动作和虚拟接口在 NAT 模式下的匹配优先级是怎么样的?

出口接口为 NAT 模式时，实际上执行的是 PAT 操作。安全策略中的 PAT 优先级高于接口上的。如果配置策略以应用 PAT，且出口接口处于 NAT 模式，则基于策略的 PAT 设置会覆盖基于接口的 NAT。

6. 安全策略中的 QoS 优先级和基于用户的 QoS 授权优先级是区别?

安全策略中的 QoS 优先级高于基于用户的 QoS。例如：定义了一个名为 Mike 的用户，其 QoS 是 200KB-CoS:7。同时配置了一个基于源用户(Mike)的安全策略，其 QoS 是 500KB-CoS:2。当 Mike 这个用户登陆后，如果匹配到那条安全策略,则在 DPF-Series 设备设备中根据安全策略定义的 QoS 进行处理。

7. 安全策略中引用计划的作用是什么?

在安全策略中可以引用某一个预先定义的计划配置(系统配置->对象->计划)。这种引用的作用是只有在这个计划时间内,这条安全策略才是有效的,而其他时间内这条安全策略是无效的。

8. 安全策略中引用安全配置的作用是什么？

因为在入侵检测配置中我们会定义多种不同防攻击，入侵检测或者过滤等“安全配置”，这些“安全配置”是需要在安全策略定义中引用了才会起作用。也就是说，一个 IP 报文只有匹配了动

作是 permit 的安全策略，且引用了相关的 “安全配置”，这个 IP 报文才会进行入侵检测配置中定义的各种防攻击、入侵检测、过滤等安全操作。

13 DHCP

13.1 简介

“动态主机配置协议” (DHCP) 的设计目的是通过自动为网络中的主机分配 TCP/IP 设置，来减少对网络管理员的需求。DHCP 会代替管理员自动为网络中的每台机器分配、配置、跟踪和更改 (必要时) 所有 TCP/IP 设置。此外，DHCP 还可以确保不使用重复地址、重新分配未使用的地址，并且可以自动为主机连接的子网分配适当的 IP 地址。

DPF-Series 设备支持不同的 DHCP 角色：

◆ **DHCP 服务器**

DPF-Series 设备可以充当 DHCP 服务器，为任意区段内的虚拟接口上的主机 (充当 DHCP 客户端) 动态分配 IP 地址。

◆ **DHCP 中继代理**

DPF-Series 设备可以充当 DHCP 中继代理，接收来自 DHCP 服务器的 DHCP 信息，然后将这些信息转交给任意区段内的任意虚拟接口连接的主机。

注意： 同一个虚拟接口上只能配置一个 DHCP 角色。例如，不能将同一虚拟接口同时配置为 DHCP 中继代理和服务器。另外，同一台 DPF-Series 设备的不同接口可以充当不同的 DHCP 角色。

13.2 DHCP 服务器

当 DPF-Series 设备用作 DHCP 服务器时，其接口可以工作于“路由”模式，亦可以工作于“透明”模式。当处于“路由”模式，此接口的 IP 地址就是DHCP 服务器地址；当处于“透明”模式，使用 DPF-Series 设备的 Layer2 IP 地址作为 DHCP 服务器地址。充当 DHCP 服务器时， DPF-Series 设备以两种模式分配 IP 地址和子网掩码：

◆ **在“动态”模式下**

充当 DHCP 服务器的 DPF-Series 设备会将地址池中的 IP 地址分配 (或“租借”) 给 DHCP 客户端主机。可在一定时间内租用该 IP 地址，也可无限期租用，直到客户端放弃该 IP 地址为止。

◆ **在“绑定”模式下**

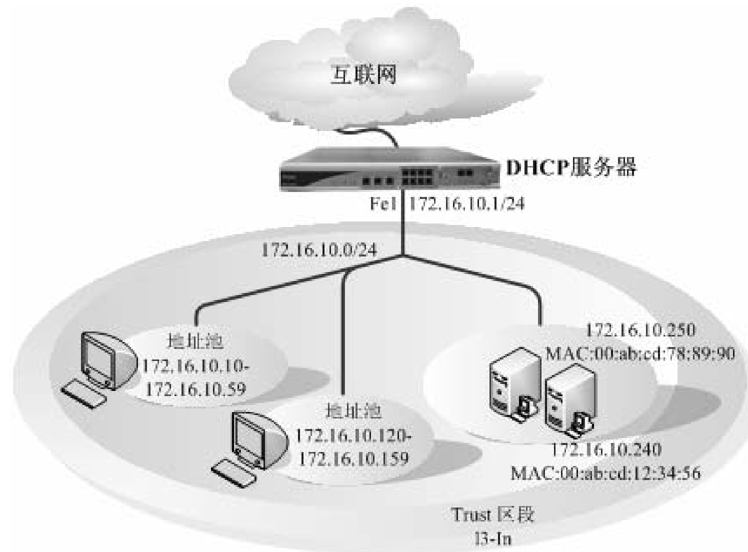
特定客户端每次联机时，DPF-Series 设备都会从地址池中专门为其分配一个指定的 IP 地址，这里是将该客户端主机的 MAC 地址和某个特定的 IP 地址绑定起来实现的。

范例: DPF-Series 设备作为 DHCP 服务器

用 DHCP 将 Trust 区段内的 172.16.10.0/24 网络分成两个 IP 地址池。

- ◆ 172.16.10.10 ～ 172.16.10.59
- ◆ 172.16.10.120 ～ 172.16.10.159

DHCP 服务器将动态分配所有 IP 地址，只有两个服务器使用预留 IP 地址。虚拟接口 vif1 绑定到 Trust 区段，其 IP 地址为 172.16.10.1/24。



CLI

1. 接口

   set vif vif1 zone l3-in
   set vif vif1 ip 172.16.10.1 netmask 255.255.255.0
   set vif vif1 filters enable web,telnet,ping

2. 动态DHCP池

   set vif vif1 dhcp mode server
   set vif vif1 dhcp server ippool ip 172.16.10.10 172.16.10.59 netmask 255.255.255.0 dns1 202.96.134.133 dns2 202.96.128.68 gateway 172.16.10.1 lease 86400
   set vif vif1 dhcp server ippool ip 172.16.10.120 172.16.10.159 netmask 255.255.255.0 dns1 202.96.134.133 dns2 202.96.128.68 gateway 172.16.10.1 lease 86400

3. DHCP绑定IP

   set vif vif1 dhcp server ipbind ip 172.16.10.240 mac 00-ab-cd-12-34-56 netmask 255.255.255.0 dns1 202.96.134.133 dns2 202.96.128.68 gateway 172.16.10.1 lease 86400
   set vif vif1 dhcp server ipbind ip 172.16.10.250 mac 00-ab-cd-78-89-90 netmask 255.255.255.0 dns1 202.96.134.133 dns2 202.96.128.68 gateway 172.16.10.1 lease 86400

4. 策略

   firewall set policy from ANY to ANY src-addr ANY dst-addr ANY service ANY action permit status enable

WEB 配置

WEB 的配置与 CLI 的配置相对应：

1. 接口

   进入 **网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)->Vif1**，允许web , ping telnet 管理。修改 zone 为 l3-in，添加 IP 地址为 172.16.10.1/24

修改虚拟接口					
虚接口名称	vif1	物理口/汇聚接口	lan1	有效	⊙ 是 ○ 否
VLAN	1	区域	l3-in		
加VLAN标签	☐	工作模式	透明模式		
报文允许	☑ web ☑ telnet ☐ ssh ☑ ping ☐ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

图54.接口配置

虚拟接口 新增

序号	名称	物理接口/汇聚口	VLAN	IP地址1/掩码	工作模式	区域	有效	操作
共 9 条记录 当前第 1 页								
1	vif0	lan0	1		透明模式	l2-in	是	
2	vif1	lan1	1		路由模式	l3-in	否	
3	vif2	lan2	1		路由模式	office	否	修改
4	vif3	lan3	1		路由模式	l3-out	否	
5	vif4	lan4	1		透明模式	l2-in	是	
6	vif5	lan5	1		透明模式	l2-in	是	
7	vif6	lan6	1		透明模式	l2-in	是	
8	vif7	lan7	1		透明模式	l2-in	是	
9	vif9	wan0	1		透明模式	l2-in	是	

图55.查看接口配置

2. 动态 DHCP 池

进入 **网络配置(NETWORK)->Protocols->DHCP**，如下图：

D-Link 友讯网络　系统名称：DPF-500　当前管理员：root

DPF-500 | 系统配置管理 | 网络配置 | 安全区域 | 网络接口 | WLAN | 路由配置 | VLAN | 网络协议 | 安全 | IM/P2P/L7 | 服务控制 | 用户 | 虚拟专用网 | 系统监控和日志

地址解析协议 | DHCP | DNS设置 | DNS缓存 | SNTP设置

DHCP

虚接口	模式	操作
共 9 条记录		
vif0	关闭	
vif1	关闭	
vif2	关闭	
vif3	关闭	
vif4	关闭	
vif5	关闭	
vif6	关闭	
vif7	关闭	
vif9	关闭	

图56.动态DHCP池

进入 vif1 配置 DHCP参数，在弹出菜单中选择“**Server**”

DHCP的模式------------虚接口 vif0	
模式	⊙ 关闭 ○ 中继代理 ○ 服务器
提交	

图57.动态DHCP池

点击“**Apply**”按钮后， **Detail** 按钮会变成可用。单击“**Detail**”后可以配置 DHCP 的 IP Pool、IP Binding 和 IP Relay 等选项。

DHCP的服务模式-----------虚接口 vif0

IP地址池		新增
开始IP	结束IP	操作

IP 绑定		新增
IP地址	MAC 地址	操作

中继代理		新增
中继代理地址	掩码	操作

返回

图58.动态DHCP池

配置 DHCP IP Pool，地址段为 172.16.10.10-172.16.10.59 和 172.16.10.120-172.16.10.159，默认的 Lease Time 为 3 天，网关、DNS、WINS、POP3 等参数属于可选项，可以按需求来进行配置。

地址解析协议 | DHCP | DNS设置 | DNS缓存 | SNTP设置

新增DHCP IP地址池 提交 取消 返回

开始IP	172.16.10.10	结束IP	172.16.10.59
租期	○ 无时间限制 ⊙ 3 天 0 小时 0 分钟		
网关	172.16.10.1	子网掩码	255.255.255.0
域名服务器#1	202.96.134.133	域名服务器#2	202.96.128.68
域名服务器#3		域名	
WINS#1		WINS#2	
SMTP		POP3	
NIS#1		NIS#2	

图59.动态DHCP池

配置好的 DHCP IP Pool 如下图：

地址解析协议 | DHCP | DNS设置 | DNS缓存 | SNTP设置

DHCP的服务模式-----------虚接口 vif0

IP地址池		新增
开始IP	结束IP	操作
172.16.10.10	172.16.10.59	
172.16.10.120	172.16.10.159	

IP 绑定		新增
IP地址	MAC 地址	操作

中继代理		新增
中继代理地址	掩码	操作

返回

图60.动态DHCP池

3. DHCP 绑定 IP

将 IP 和 MAC 进行绑定，任何时候这个主机将自动分配到一个固定的 IP 地址，这里是将 172.16.10.240 和
00-ab-cd-12-34-56

地址解析协议 | DHCP | DNS设置 | DNS缓存 | SNTP设置

新增DHCP IP绑定　提交　取消　返回

IP地址	172.16.10.240	MAC地址	00 - ab - cd - 12 - 34 - 56
租期	⦿ 无时间限制 ○ 1 天 0 小时 0 分钟		
网关	172.16.10.1	子网掩码	255.255.255.0
域名服务器#1	202.96.134.133	域名服务器#2	202.96.128.68
域名服务器#3		域名	
WINS#1		WINS#2	
SMTP		POP3	
NIS#1		NIS#2	

图61.DHCP绑定IP

同理将 172.16.10.245 和 00-ab-cd-78-89-90 进行绑定。配置后结果如下：

DHCP的服务模式-----------虚接口 vif0

IP地址池　新增

开始IP	结束IP	操作
172.16.10.10	172.16.10.59	
172.16.10.120	172.16.10.159	

IP 绑定　新增

IP地址	MAC 地址	操作

中继代理　新增

中继代理地址	掩码	操作

返回

图62.DHCP绑定IP

4. 策略

进入 **安全(SECURITY)-> 安全策略(Policies)->新增(Create New)**，配置一条 permit all 的全局策略。

安全策略: Global

安全策略　全选　提交　新增　清除

序号	源地址/用户/地址簿	目的地址/用户/地址簿	定时计划	安全配置	服务	匹配计数	动作	状态	操作
共 2 条记录 共 1 页 当前第 1 页									页码:
1	ANY	ANY			ANY	0	permit	☑	
2	1.2.2.7-1.2.2.126	ANY			FTP	0	deny	☑	

图63.策略

13.3 DHCP 中继代理

充当 DHCP 中继代理时，DPF-Series 设备负责在一个区段内的主机与另一个区段内的 DHCP 服务器之间转发 DHCP 请求和分配信息。当 DPF-Series 设备用作 DHCP 中继代理时，其接口可以工作于“路由”模式，亦可以工作于“透明”模式。当处于“路由”模式，此接口的 IP 地址就是 DHCP 中继代理地址；当处于“透明”模式，使用 DPF-Series 设备的 Layer2 IP 地址作为 DHCP 中继代理地址。中继代理将 DHCP 客户端的地址请求报文发送到已配置的 DHCP 服务器上。随后，中继代理将收到的服务器响应转发给客户端。

范例: DPF-Series 设备作为 DHCP 中继代理

在本例中，DPF-Series 设备从 IP 地址为 194.2.9.10 的 DHCP 服务器中接收 DHCP 信息，而后将其转递给 Trust 区段中的主机。主机从 DHCP 服务器上定义的 IP 池中租借 IP 地址。地址范围是 180.10.10.2-180.10.10.250。该 DHCP 服务器位于 Untrust 区段路由器之后。接口 vif1 被绑定到 Trust 区段，IP 地址为 180.10.10.1/24。接口 vif3 被绑定到 Untrust 区段中， IP 地址为 1.1.1.1/24。



CLI

1. 接口

   set vif vif1 zone l3-in
   set vif vif3 zone l3-out
   set vif vif1 ip 180.10.10.1 netmask 255.255.255.0
   set vif vif3 ip 1.1.1.1 netmask 255.255.255.0
   set vif vif1 filters enable web,telnet,ping
   set vif vif3 filters enable web,telnet,ping

2. DHCP中继代理

   set vif vif1 dhcp mode relay
   set vif vif1 dhcp relay target 192.2.9.10

3. 路由

   set route ip 0.0.0.0 0.0.0.0 1.1.1.250

4. 策略

   firewall set policy from ANY to ANY src-addr ANY dst-addr ANY service ANY action permit status enable
   save

WEB 配置

WEB 的配置与 CLI 的配置相对应：

1. 接口

   进入 **网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)->Vif1**，允许web , ping,telnet 管理。修改 zone 为l3-in，添加 IP 地址为 180.10.10.1/24

修改虚拟接口					提交 取消 返回
虚接口名称	vif1	物理口/汇聚接口	lan1	有效	○ 是 ⊙ 否
VLAN	1	区域	l3-in		
加VLAN标签	☐	工作模式	路由模式		
地址转换	☐ 启用				
报文允许	☑ web ☑ telnet ☐ ssh ☑ ping ☐ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

图64.vif

同理添加 vif3 的 IP 地址 1.1.1.1/24，如下图：

虚拟接口 新增

共 9 条记录 当前第 1 页

序号	名称	物理接口/汇聚口	VLAN	IP地址1/掩码	工作模式	区域	有效	操作
1	vif0	lan0	1		透明模式	l2-in	是	
2	vif1	lan1	1		路由模式	l3-in	否	
3	vif2	lan2	1		路由模式	office	否	
4	vif3	lan3	1		路由模式	l3-out	否	
5	vif4	lan4	1		透明模式	l2-in	是	
6	vif5	lan5	1		透明模式	l2-in	是	
7	vif6	lan6	1		透明模式	l2-in	是	
8	vif7	lan7	1		透明模式	l2-in	是	
9	vif9	wan0	1		透明模式	l2-in	是	

图65.vif(1)

2. DHCP 中继代理

进入 vif1 配置 DHCP 参数，在弹出菜单中选择“**Relay**”

DHCP的模式------------虚接口 vif1	
模式	○ 关闭 ⊙ 中继代理 ○ 服务器
	提交 高级配置

图66.DHCP中继代理

单击“**Detail**”进入配置菜单

中继代理参数设置 虚接口: vif1	提交 取消
中继代理跳数：	5

中继代理目的地址设置	新增 返回
目的地址	操作

图67.DHCP中继代理

添加 DHCP Server的 IP 地址

中继代理参数设置 虚接口: vif1	提交 取消
中继代理跳数：	5

中继代理目的地址设置	新增 返回
目的地址	操作
192.2.9.10	

图68.DHCP中继代理

3. 路由

进入 **网络配置(NETWORK)->路由配置(Routing)->网络路由(Static Routing)->新增(Create New)**，添加一条到 1.1.1.250 的默认路由：

新增网络路由表			提交 取消 返回
IP地址	0.0.0.0	子网掩码	0.0.0.0
网关/ISP	1.1.1.250		
*IP地址 0.0.0.0 掩码 0.0.0.0 代表缺省路由			

图69.路由

4. 策略

进入 安全(SECURITY)-> 安全策略(Policies)->新增(Create New) ，添加一条全局的 permit all 的策略。

安全策略: Global

安全策略　全选　提交　新增　清除

序号	源地址/用户/地址簿	目的地址/用户/地址簿	定时计划	安全配置	服务	匹配计数	动作	状态	操作
共 2 条记录 共 1 页 当前第 1 页									页码:
1	ANY	ANY			ANY	0	permit	☑	

图70.策略

14 网络地址转换

14.1 简介

“网络地址转换”是一种 Internet Engineering Task Force (IETF) 标准，用于允许专用网络上的多台 PC 机（使用私有地址范围，例如 10.0.x.x、192.168.x.x、172.16.0.0 – 172.31.255.255）共享单个或者多个、可全局路由的 IPv4 地址。经常部署 NAT 的一个主要原因就是 IPv4 地址日渐紧缺，另外也常用来保护内部的服务器和主机。

DPF-Series 设备提供了应用网络地址转换的多种机制。 NAT 只转换 IP 包头中的 IP 地址；PAT 是转换 IP 包头中的 IP 地址和 TCP 或 UDP 数据报头中的端口号，转换中包含源地址 (以及可选的源端口号)，或者目的地址 (以及可选的目的端口号) 等。

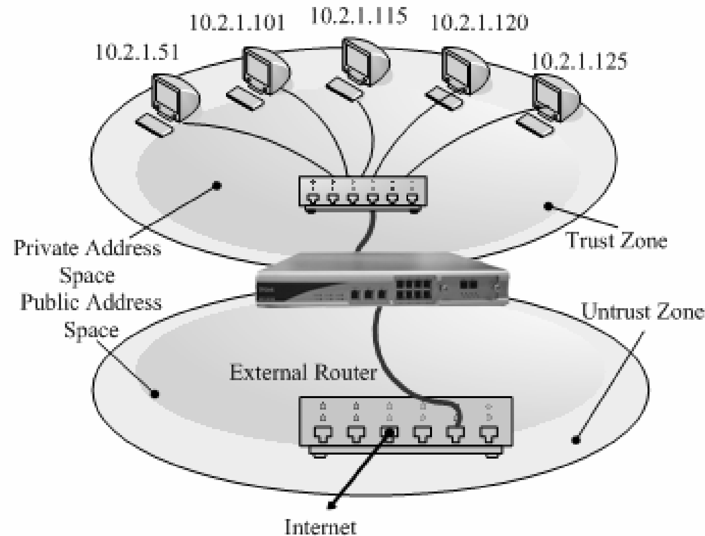


图71.网络地址转换

14.2 PAT

PAT 转换是 **单向** 转换，用于从 trust 安全区段到 untrust 区段的转换。PAT 转换也是 **多对一** 的转换，它把专用地址映射到全局地址的不同端口上，因一个 IP 地址的端口数有 65535 个，也就是说一个全局地址最多可以为 65535 个内部地址建立映射。故从理论上来说，一个全局地址就可供 6 万多个内部地址通过 PAT 连接到互联网。

DPF-Series 设备执行 PAT 转换时，将从 Trust 区段通往 Untrust 区段的外向 IP 封包包头中的两个组件进行转换：其源 IP 地址和源端口号。 DPF-Series 设备用 Untrust 区段接口的 IP 地址（或者配置的 IP 池里的地址）替换发端主机的源 IP 地址。另外，它用另一个由 DPF-Series 设备生成的任意端口号替换源端口号。当回复封包到达 DPF-Series 设备时，该设备转换内向封包的 IP 包头中的两个组件：目的地地址和端口号，它们被转换回初始号码。 DPF-Series 设备于是将封包转发到其目的地。

DPF-Series 设备的 PAT 转换有两种类型：

◆ 基于策略的 PAT：在策略中引用 PAT，那么匹配此策略的报文将执行 PAT转换。

- 基于接口的 PAT：在出口接口中配置 PAT，此时接口从路由模式变成 **NAT 模式**。那么通过此接口出去的报文将执行 PAT 转换。

执行 PAT 时，已转换地址来自 IP 池。IP 池里的地址可以配置为出口接口的 IP 地址，或者与出口接口同一网段的 IP 地址（或者一段地址）。在出口接口配置 PAT 时，如果不选择 IP 池，那么将报文的源 IP 转换成出口接口的 IP，如果选择了 IP 池，就将报文的源 IP 转换成 IP 池里的 IP；在策略中配置 PAT 时必须要选择一个 IP 池。

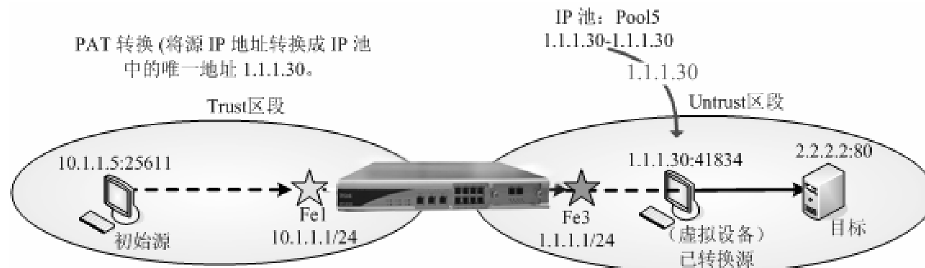
DPF-Series 设备可以从 IP 池里随机提取或提取明确的地址，也就是说，既可以从 IP 池中随机提取地址，也可以持续提取与初始源 IP 地址有关的特定地址， 这一点通过是否选择“**固定IP(Fixed IP)**”来实现。配置 PAT 转换时，如果选择了“**固定IP(Fixed IP)**”，则同一源 IP 地址的封包每次都转换成同一 IP 地址。有些协议（例如 FTP）的端口在变化，就必须要选择在“**固定IP(Fixed IP)**”。在此还有一个“**固定端口 (Fixed port)**”的选项，如果选择了“**固定端口(Fixed port)**”，则报文里的端口不被转换。

安全策略中的 PAT 优先级 **低于** 接口上的。也就是说，如果策略里配置了 PAT，出口接口也配置了 PAT，则基于接口的 PAT 设置会覆盖基于策略的 PAT。

范例：基于策略的 PAT

本例中，内网主机使用私网 IP。定义 IP 池 pool5，池里只包含单个 IP 地址 1.1.1.30。随后，在策略设置 PAT 转换，指示 DPF-Series 设备执行以下任务：

- 允许 Trust 区段中任意地址发出的 HTTP 信息流流向 Untrust 区段中的任意地址
- 将 IP 封包包头中的源 IP 地址转换成 1.1.1.30，该地址是 IP 池 pool5 中的唯一条目
- 将带有已转换源 IP 地址和端口号的 HTTP 信息流通过 FE3 发送到 Untrust 区段



CLI

1. 接口
   set vif vif1 zone l3-in
   set vif vif3 zone l3-out
   set vif vif1 ip 10.1.1.1 netmask 255.255.255.0
   set vif vif3 ip 1.1.1.1 netmask 255.255.255.0
   set vif vif1 filters enable web,telnet,ping
   set vif vif3 filters enable web,telnet,ping
2. 路由
   set route ip 0.0.0.0 0.0.0.0 1.1.1.250
3. IP pool
   firewall set pat-pool pool5 1.1.1.30 1.1.1.30
4. 策略

firewall set policy from l3-in to l3-out src-addr ANY dst-addr ANY service HTTP action pat pat-pool pool5 pat-stick-ip status enable

WEB 配置

WEB 的配置与 CLI 的配置相对应：

1. 接口

进入 **网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)->Vif1**，允许web , ping telnet 管理。修改 zone 为 l3-in，添加 IP 地址为 10.1.1.1/24

修改虚拟接口					提交 取消 返回
虚拟接口名称	vif1	物理口/汇聚接口	lan1	有效	○ 是 ◉ 否
VLAN	1	区域	l3-in		
加VLAN标签	☐	工作模式	路由模式		
地址转换	☐ 启用				
报文允许	☑ web ☑ telnet ☐ ssh ☑ ping ☐ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

图72.接口配置

同理添加 vif3 的 IP 地址 1.1.1.1/24，如下图：

虚拟接口 新增

共 9 条记录 当前第 1 页

序号	名称	物理接口/汇聚口	VLAN	IP地址1/掩码	工作模式	区域	有效	操作
1	vif0	lan0	1		透明模式	l2-in	是	
2	vif1	lan1	1		路由模式	l3-in	否	
3	vif2	lan2	1		路由模式	office	否	
4	vif3	lan3	1		路由模式	l3-out	否	
5	vif4	lan4	1		透明模式	l2-in	是	
6	vif5	lan5	1		透明模式	l2-in	是	
7	vif6	lan6	1		透明模式	l2-in	是	
8	vif7	lan7	1		透明模式	l2-in	是	
9	vif9	wan0	1		透明模式	l2-in	是	

图73.接口配置

2. 路由

进入 **网络配置(NETWORK)->路由配置(Routing)->网络路由(Static Routing)->新增(Create New)**，添加一条到 1.1.1.250 的默认路由：

新增网络路由表			提交 取消 返回
IP地址	0.0.0.0	子网掩码	0.0.0.0
网关/ISP	1.1.1.250		
*IP地址 0.0.0.0 掩码 0.0.0.0 代表缺省路由			

图74.配置路由

3. IP pool

进入**安全(SECURITY) ->NAT->IP Pool->新增(Create New)**，添加一个 IP pool。地址范围一定是和出接口同网段的 IP 地址，如下图：

新增端口转换地址池			提交 取消 返回
名称	pool5		
注释			
起始转换IP	1.1.1.30	结束转换IP	1.1.1.30

图75.IP pool

4. 策略

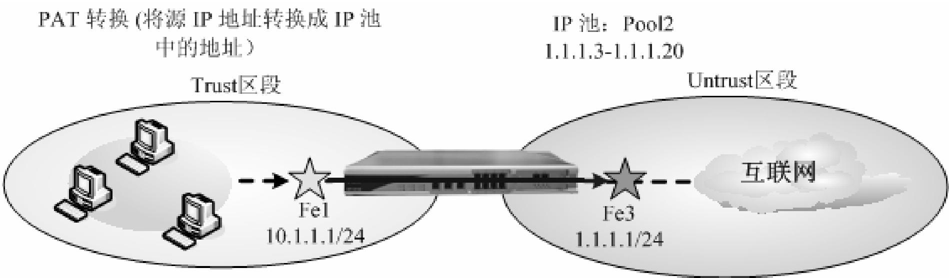
进入 **安全(SECURITY)->安全策略(Policies)->新增(Create New)**，添加一条从源区段 l3-in 到目的区段 l3-out 的策略，动作为 PAT（IP Pool 选择 pool5），允许 HTTP 服务。

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 [ ] 之前 ⦿ 最后		
安全区			
源安全区	l3-in	目的安全区	l3-out
地址/用户/地址簿			
	⦿ 源 地址 ○ 用户 ○ 地址簿		
	⦿ 目的地址 ○ 用户 ○ 地址簿		
动作	PAT	服务	HTTP
端口转换	PAT池 pool5 固定端口 ☐ 固定IP ☑		
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☐ 显示高级	

图76.策略

范例：基于接口的 PAT

本例中，Trust 区段的内网使用私网地址段 10.1.1.0/24，当内网的 PC 访问互联网时需要进行 PAT 转换。定义 IP 池 pool2，池里包含一段地址：1.1.1.3-1.1.1.20。随后，在 Untrust 区段的 FE3 接口上配置 PAT 转换，引用 pool2，并且启用“固定 IP”，使内网中同一个源 IP 转换成 IP 池中相同的地址。



CLI

1. IP pool
```
firewall set pat-pool pool2 1.1.1.3 1.1.1.20
```
2. 接口
```
set vif vif1 zone l3-in
set vif vif3 zone l3-out
set vif vif1 ip 10.1.1.1 netmask 255.255.255.0
set vif vif3 ip 1.1.1.1 netmask 255.255.255.0
set vif vif3 nat pat-pool pool2 stick-ip
set vif vif1 filters enable web,telnet,ping
set vif vif3 filters enable web,telnet,ping
```
3. 路由
```
set route ip 0.0.0.0 0.0.0.0 1.1.1.250
```

4. 策略

   firewall set policy from l3-in to l3-out src-addr ANY dst-addr ANY service ANY action permit status enable

WEB 配置

WEB 的配置与 CLI 的配置相对应：

1. IP pool

进入**安全(SECURITY) ->NAT->IP Pool->新增(Create New)**，添加一个 IP pool。如下图：

新增端口转换地址池			提交 取消 返回
名称	pool2		
注释			
起始转换IP	1.1.1.3	结束转换IP	1.1.1.20

图77. IP pool

2. 接口

进入 **网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)->Vif1**，允许web , ping telnet 管理。修改 zone 为 l3-in，添加 IP 地址为 10.1.1.1/24

修改虚拟接口					提交 取消 返回
虚接口名称	vif1	物理口/汇聚接口	lan1	有效	○ 是 ⊙ 否
VLAN	1	区域	l3-in		
加VLAN标签	☐	工作模式	路由模式		
地址转换	☐ 启用				
报文允许	☑ web ☑ telnet ☐ ssh ☑ ping ☐ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

图78. 接口配置

再添加 vif3 的 IP 地址 1.1.1.1/24，然后配置 PAT 转换，地址池引用 pool2(如果不选择任何 IP 池，内网地址将被转换为 vif3 的接口 IP：1.1.1.1)；选择**"固定 IP(Fixed IP)"**。如下图：

修改虚拟接口					提交 取消 返回
虚接口名称	vif3	物理口/汇聚接口	lan3	有效	○ 是 ⊙ 否
VLAN	1	区域	l3-out		
加VLAN标签	☐	工作模式	路由模式		
地址转换	☑ 启用				
端口转换	PAT池 pool5 固定端口 ☐ 固定IP ☐				
报文允许	☑ web ☑ telnet ☐ ssh ☑ ping ☐ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

图79. 接口pat配置

3. 路由

进入 **网络配置(NETWORK)->路由配置(Routing)->网络路由(Static Routing)->新增(Create New)**，添加一条到 1.1.1.250 的默认路由：

新增网络路由表			提交 取消 返回
IP地址	0.0.0.0	子网掩码	0.0.0.0
网关/ISP	1.1.1.250		
*IP地址 0.0.0.0 掩码 0.0.0.0 代表缺省路由			

图80.配置路由

4. 策略

进入 **安全(SECURITY)->安全策略(Policies)->新增(Create New)**，添加一条从源区段 l3-in 到目的区段 l3-out 的策略，动作为 PERMIT。

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 之前 ⊙ 最后		
安全区			
源安全区	l3-in	目的安全区	l3-out
地址/用户/地址簿			
⊙ 源 地址 ○ 用户 ○ 地址簿			
⊙ 目的地址 ○ 用户 ○ 地址簿			
动作	PERMIT	服务	ANY
日志	□ log		
防病毒	□ 防病毒		
使能	⊙ 启用 ○ 禁用	□ 显示高级	

图81.策略

14.3 NAT

NAT 转换是 **一对一、双向** 的转换，可以将从 Trust 区段通往 Untrust 区段的外向封包中的源 IP 地址进行转换，或者将从 Untrust 区段通往 Trust 区段的内向封包中的目的 IP 地址进行转换。

进行源 IP 转换时，DPF-Series 设备用 NAT 池里配置的对应地址（与 Untrust 区段接口同一网段的 IP 地址）替换发端主机的源 IP 地址。当回复封包到达 DPF-Series 设备时，该设备转换内向封包的 IP 包头中目的地地址，它被转换回初始号码；DPF-Series 设备于是将封包转发到其目的地。进行目的 IP 转换时，DPF-Series 设备用 NAT 池里配置的对应地址（与 Trust 区段接口同一网段的 IP 地址）替换发端主机的目的 IP 地址。当回复封包到达 DPF-Series 设备时，该设备转换外向封包的 IP 包头中源地地址，它被转换回初始号码；DPF-Series 设备于是将封包转发到其目的地。

范例: NAT 转换

以下范例说明了 Trust 区段受 NAT 模式下的 DPF-Series 设备保护。Trust 区段中的服务器和客服机的 IP（10.2.1.0/24）被转换成出口网段中的 IP（1.1.1.0/24）。Trust 和 Untrust 区段都在 in-vr 路由选择域中。



CLI

1. 接口

set vif vif1 zone l3-in
set vif vif3 zone l3-out
set vif vif1 ip 10.2.1.1 netmask 255.255.255.0
set vif vif3 ip 1.1.1.1 netmask 255.255.255.0
set vif vif1 filters enable web,telnet,ping
set vif vif3 filters enable web,telnet,ping

2. NAT 池

firewall set nat natname nat-start 1.1.1.5 nat-end 1.1.1.7 host-start 10.2.1.5 host-end 10.2.1.7

3. 路由

set route ip 0.0.0.0 0.0.0.0 1.1.1.250

4. 策略

firewall set policy from ANY to ANY src-addr ANY dst-addr ANY service ANY action permit status enable

WEB 配置

WEB 步骤如下，web 的配置与上面命令行的配置相对应：

1. 接口

进入 **网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)->Vif1**，修改 zone 为 l3-in，如下：

虚拟接口 | 物理接口 | 管理接口 | 二层接口 | 汇聚接口

修改虚拟接口 提交 取消 返回

虚接口名称	vif1	物理口/汇聚接口	lan1	有效	○ 是 ⦿ 否
VLAN	1	区域	l3-in		
加VLAN标签	☐	工作模式	路由模式		
地址转换	☐ 启用				
报文允许	☑ web ☑ telnet ☐ ssh ☑ ping ☐ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

图82.接口配置

同理配置 vif3，如下：

修改虚拟接口 提交 取消 返回

虚接口名称	vif3	物理口/汇聚接口	lan3	有效	○ 是 ⦿ 否
VLAN	1	区域	l3-out		
加VLAN标签	☐	工作模式	路由模式		
地址转换	☐ 启用				
报文允许	☑ web ☑ telnet ☐ ssh ☑ ping ☐ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

图83.接口配置

为 vif1 配置 IP 地址：10.2.1.1/24,如下：

新增IP 虚接口VIF:vif1 提交 取消 返回

IP地址	10.2.1.1/24
子网掩码	255.255.255.0

图84.配置 IP

为 vif3 配置 IP 地址：1.1.1.1/24,如下：

新增IP 虚接口VIF:vif3	提交 取消 返回
IP地址	1.1.1.1
子网掩码	255.255.255.0

图85.配置 IP

2. NAT 池

进入 **安全(SECURITY)->NAT->新增(Create New)**，添加 NAT 池，如下图：

新增端口转换地址池			提交 取消 返回
名称	natname		
注释			
起始转换IP	10.2.1.5	结束转换IP	1.1.1.5

图86.nat

3. 路由

进入 **网络配置(NETWORK)->路由配置(Routing)->网络路由(Static Routing)->新增(Create New)**，添加一条到 1.1.1.250 的默认路由：

新增网络路由表			提交 取消 返回
IP地址	0.0.0.0	子网掩码	0.0.0.0
网关/ISP	1.1.1.250		
*IP地址 0.0.0.0 掩码 0.0.0.0 代表缺省路由			

图87.路由

4. 策略

进入 **安全(SECURITY) ->安全策略(Policies)->新增(Create New)**，添加一条全局的 permit all的策略：

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 之前 ⦿ 最后		
安全区			
源安全区	ANY	目的安全区	ANY
地址/用户/地址簿			
	⦿ 源 地址 ○ 用户 ○ 地址簿		
	⦿ 目的地址 ○ 用户 ○ 地址簿		
动作	PERMIT	服务	ANY
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☐ 显示高级	

图88.策略

14.4 服务映射（SERVICE MAPPING）

服务映射是从一个（IP地址+端口号）到另一个（IP地址+端口号）的 **一对一** 映射，是 **单向** 的转换。DPF-Series 设备将从 Untrust 区段通往 Trust 区段的内向封包中的两个组件进行转换: 其目的 IP 地址和目的端口号。DPF-Series 设备用 Trust 区段接口的 IP 地址（或者同一网段的 IP 地址）替换发端主机的目的 IP 地址；另外，它用预先配置的端口号替换目的端口号。当回复封包到达 DPF-Series 设备时，该设备转换外向封包的 IP 包头中的两个组件: 源地址和源端口号，它们被转换回初始号码。DPF-Series 设备于是将封包转发到其目的地。

范例：服务映射

为了保护内部服务器，提供给外部用户的地址（和端口号）可以不是内部服务器真正的地址，而是告诉外部用户一个公网地址（和其它端口号），内部通过 DPF-Series 设备来实现地址和端口转换。对于外部用户来说是完全透明的。

本例中，提供给外部用户的 WEB 服务器地址为 1.1.1.5（port：8181）。在 DPF-Series 设备上，将目的地址为 Untrust 区段中 1.1.1.5 的内向 HTTP 信息流发送到 Trust 区段地址为 10.1.1.5 的 Web 服务器。

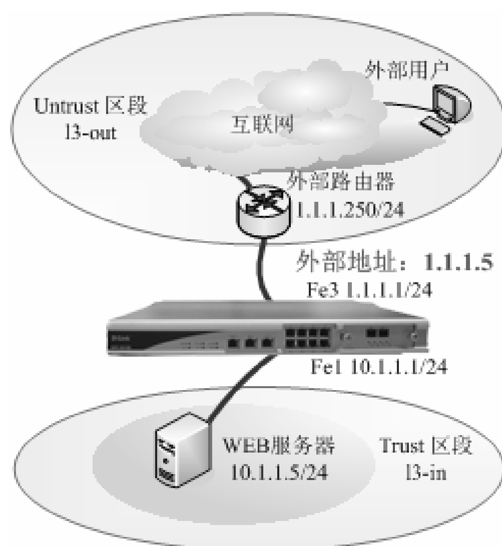


图89.服务映射

CLI

1. 接口

```
set vif vif1 zone l3-in
set vif vif3 zone l3-out
set vif vif1 ip 10.1.1.1 netmask 255.255.255.0
set vif vif3 ip 1.1.1.1 netmask 255.255.255.0
set vif vif1 filters enable web,telnet,ping
set vif vif3 filters enable web,telnet,ping
```

2. 路由

```
set route ip 0.0.0.0 0.0.0.0 1.1.1.250
```

3. servie mapping

```
firewall set service-mapping name 1.1.1.5 mstart-port 8181 mend-port 8181 protocol tcp host-ip 10.1.1.5 hstart-port 80 hend-port 80
```

4. 策略

```
firewall set policy from ANY to ANY src-addr ANY dst-addr ANY service ANY action permit
status enable
save
```

WEB 配置

WEB 的配置与 CLI 的配置相对应：

1. 接口

进入 **网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)->Vif1**，允许web , ping,telnet 管理。修改 zone 为l3-in，添加 IP 地址为 10.1.1.1/24

虚拟接口 | 物理接口 | 管理接口 | 二层接口 | 汇聚接口

修改虚拟接口 提交 取消 返回

虚拟接口名称	vif1	物理接口/汇聚接口	lan1	有效	○ 是 ⊙ 否
VLAN	1	区域	l3-in		
加VLAN标签	☐	工作模式	路由模式		
地址转换	☐ 启用				
报文允许	☑ web ☑ telnet ☐ ssh ☑ ping ☐ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

图90.接口配置

同理添加 vif3 的 IP 地址 1.1.1.1/24，如下图：

虚拟接口 新增

序号	名称	物理接口/汇聚接口	VLAN	IP地址1/掩码	工作模式	区域	有效	操作
共 9 条记录 当前第 1 页								
1	vif0	lan0	1		透明模式	l2-in	是	
2	vif1	lan1	1		路由模式	l3-in	否	
3	vif2	lan2	1		路由模式	office	否	
4	vif3	lan3	1		路由模式	l3-out	否	
5	vif4	lan4	1		透明模式	l2-in	是	
6	vif5	lan5	1		透明模式	l2-in	是	
7	vif6	lan6	1		透明模式	l2-in	是	
8	vif7	lan7	1		透明模式	l2-in	是	
9	vif9	wan0	1		透明模式	l2-in	是	

图91.接口配置

2. 路由

进入 **网络配置(NETWORK)->路由配置(Routing)->网络路由(Static Routing)->新增(Create New)**，添加一条到 1.1.1.250 的静态路由：

新增网络路由表 提交 取消 返回

IP地址	0.0.0.0	子网掩码	0.0.0.0
网关/ISP	1.1.1.250		
*IP地址 0.0.0.0 掩码 0.0.0.0 代表缺省路由			

图92.配置路由

3. Service Mapping

进入 **安全(SECURITY)-> NAT -> Service Mapping->新增(Create New)**，选择需要映射的 IP 和初始端口号和外部的端口号，这里选择的是 80——> 8181。
【80 是内部服务器的 HTTP 端口，8181 是提供给外部用户的端口。也可以不进行端口映射，这时，内部端口和外部端口都是 80 】

新增服务映射		提交 取消 返回	
名称	name		
注释			
协议号	TCP		
初始IP	10.1.1.5	转换IP	1.1.1.5
初始端口	80 - 80		
转换端口	8181 - 8181		

图93.service mapping

4. 策略

进入 **安全(SECURITY)-> 安全策略(Policies)->新增(Create New)**，添加一条全局的 permit all 的策略

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 ____ 之前 ⦿ 最后		
安全区			
源安全区	ANY	目的安全区	ANY
地址/用户/地址簿			
	⦿ 源 地址 ○ 用户 ○ 地址簿		
	⦿ 目的地址 ○ 用户 ○ 地址簿		
动作	PERMIT	服务	ANY
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☐ 显示高级	

图94.策略

14.5 负载均衡 (LOAD BALANCE)

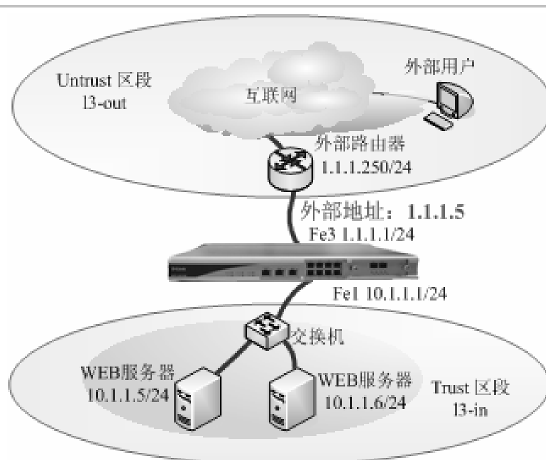
服务映射是 **一对多** 的映射、是 **单向** 的转换。可以将某个来自外部（IP 地址+端口号）的信息流随机映射到最多 8 个（IP 地址+端口号）中的一个，从而达到负载分流和均衡的效果。和服务映射类似，所不同的是可以把一个 IP 地址和端口(或者端口范围)转换成多个 IP 地址（同一子网）和端口(或者端口范围)。在多个内部 IP 地址(主机)之间可以设置均衡的方式，这样就可以把一个 IP 地址上的流量均衡到内部多个 IP 地址的主机上。

对于内部主机，DPF-Series 设备支持健康侦测。如果配置的内部主机都是存活的，则在多个主机间均衡流量，如果一旦探测到某个主机失效，则在剩下的主机间均衡，如果先前失效的主机恢复了，则又参加到均衡队伍中。

范例：负载均衡

为了保护内部服务器和减轻内部服务器的负担。一般来说，提供给外部用户的地址（和端口号）可以不是内部服务器真正的地址；而是告诉外部用户一个公网地址（和其它端口号），内部通过 DPF-Series 设备来实现地址转换和负载均衡。对于外部用户来说是完全透明的。

某软件公司创建了一个公司网站，提供给外部用户的地址为 1.1.1.5（port：8089）。所以在 DPF-Series 设备上将目的地址为 Untrust 区段中 1.1.1.5 的内向 HTTP 信息流转换到 Trust 区段地址为 10.1.1.5 或者 10.1.1.6 的 Web 服务器。内部主机的端口号为 80 。



CLI

1. 接口
   set vif vif1 zone l3-in
   set vif vif3 zone l3-out
   set vif vif1 ip 10.1.1.1 netmask 255.255.255.0
   set vif vif3 ip 1.1.1.1 netmask 255.255.255.0
   set vif vif1 filters enable web,telnet,ping
   set vif vif3 filters enable web,telnet,ping
2. 路由
   set route ip 0.0.0.0 0.0.0.0 1.1.1.250
3. Loadbanlace
   firewall set balance-mapping Load Balance web-load 1.1.1.5 start-port 8089 end-port 8089 protocol tcp
   firewall set balance-mapping Load Balance host host-ip 10.1.1.5 start-port 80 end-port 80 sharing 3 track enable
   firewall set balance-mapping Load Balance host host-ip 10.1.1.6 start-port 80 end-port 80 sharing 5 track enable
4. 策略
   firewall set policy from ANY to ANY src-addr ANY dst-addr ANY service ANY action permit status enable

WEB 配置

WEB 的配置与 CLI 的配置相对应：

1. 接口

   进入 **网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)->Vif1**，允许web , ping,telnet 管理。修改 zone 为 l3-in，添加 IP 地址为 10.1.1.1/24

虚拟接口 | 物理接口 | 管理接口 | 二层接口 | 汇聚接口

修改虚拟接口　　提交　取消　返回

虚接口名称	vif1	物理口/汇聚接口	lan1	有效	○是 ⊙否
VLAN	1	区域	l3-in		
加VLAN标签	☐	工作模式	路由模式		
地址转换	☐ 启用				
报文允许	☑ web ☑ telnet ☐ ssh ☑ ping ☐ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

图95.接口配置

同理添加 vif3 的 IP 地址 1.1.1.1/24，如下图：

虚拟接口　　新增

序号	名称	物理接口/汇聚口	VLAN	IP地址1/掩码	工作模式	区域	有效	操作
共 9 条记录 当前第 1 页								
1	vif0	lan0	1		透明模式	l2-in	是	
2	vif1	lan1	1		路由模式	l3-in	否	
3	vif2	lan2	1		路由模式	office	否	
4	vif3	lan3	1		路由模式	l3-out	否	
5	vif4	lan4	1		透明模式	l2-in	是	
6	vif5	lan5	1		透明模式	l2-in	是	
7	vif6	lan6	1		透明模式	l2-in	是	
8	vif7	lan7	1		透明模式	l2-in	是	
9	vif9	wan0	1		透明模式	l2-in	是	

图96.接口配置

2. 路由

进入 **网络配置(NETWORK)->路由配置(Routing)->网络路由(Static Routing)->新增(Create New)**，添加一条到 1.1.1.250 的静态路由：

新增网络路由表　　提交　取消　返回

IP地址	0.0.0.0	子网掩码	0.0.0.0
网关/ISP	1.1.1.250		
*IP地址 0.0.0.0 掩码 0.0.0.0 代表缺省路由			

图97.配置路由

3. Load Balance

进入**安全(SECURITY)-> NAT ->Load Balance->新增(Create New)**，创建 Load Balance。输入外部 IP，选择需要映射协议和端口号范围。这里选择的协议是 TCP，端口号是 8089。如下：

新增负载均衡映射　　提交　取消　返回

名称	web-load		
注释			
转换IP	1.1.1.5	协议号	TCP
转换端口	8089 - 8089		

图98.load balance

点击“**Apply**”按钮，创建成功，返回 Load Balance 的主页面，可以看到刚才的配置，如下：

负载均衡映射　　新增

序号	名称	转换IP	转换端口	协议号	使能	操作
共 1 条记录						
1	web-load	1.1.1.5	8089-8089	tcp	禁用	

图99.load balance

然后点击上图的蓝色框所示的“Host List”按钮，添加主机成员。

【最多可以添加 8 个主机成员，所有主机成员的“Load balance”的总和必须是 8 】

添加第一个（10.1.1.5）主机成员，“Load balance”为 3 ，并启用健康侦测功能。

新增主机列表			提交 取消 返回
初始IP	10.1.1.5	负载均衡映射	3
端口	80 - 80		
侦测允许	☑		

图100. load balance

同理添加第二个（10.1.1.6）主机成员，“Load balance”为 5 ，并启用健康侦测功能。

4. 策略

进入 **安全(SECURITY)-> 安全策略(Policies)->新增(Create New)** ，添加一条全局的 permit all 的策略

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 之前 ⊙ 最后		
安全区			
源安全区	ANY	目的安全区	ANY
地址/用户/地址簿			
	⊙ 源 地址 ○ 用户 ○ 地址簿		
	⊙ 目的地址 ○ 用户 ○ 地址簿		
动作	PERMIT	服务	ANY
日志	☐ log		
防病毒	☐ 防病毒		
使能	⊙ 启用 ○ 禁用	☐ 显示高级	

图101. 策略

15 用户认证

15.1 简介

DPF-Series 设备支持 Web 认证和 802.1x 认证。除本地数据库外，DPF-Series 设备还支持外部 POP3 服务器、域名服务器、RADIUS 和 LDAP 服务器。可使用各种类型的认证服务器对 auth 用户进行认证。同时 DPF-Series 设备支持 RADIUS 和 LDAP 服务器计费方式，可以按时间和流量来计费。另外 DPF-Series 设备还可以设置静态用户，该种用户不需要进行认证，而是开机后直接可以访问网络资源。

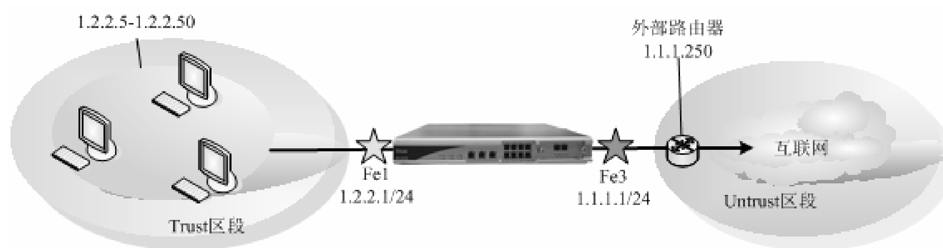
DPF-Series 设备对用户身份认证的同时也可以对用户做绑定检查。可对用户的 PC 机的主机名、IP 地址、MAC 地址、接入的 VLAN ID、接入的物理端口号等各种组合进行严格检查。在所有访问过程中都会进行严格的终端绑定检查，以保证用户的合法性。

DPF-Series 设备对于用户认证的方法、授权和计费都是基于策略进行的。根据网络的实际需要，针对不同的用户或者用户组，可以定制多种认证和管理的策略，进行更加有效和有针对性地管理配置。不是所有接入网络的用户都需要认证，而是根据实际需要决定哪些用户或服务需要进行认证。举个例子，在 DPF-Series 设备上制定这样的安全策略：IP 地址是 10.0.0.5-10.0.0.9 的用户访问 IP 为 10.0.0.10 的 FTP 服务时需要进行 Web 认证，而在访问 IP 为 10.0.0.11 的 Web 服务时采用 802.1x 认证。也就是说，只有符合上述安全策略时，用户必须先进行认证，才能获得相应的网络服务。而其他所有的访问都不需要认证。

对于认证、授权、计费的方法以及用户组的信息，DPF-Series 设备已经设置了一些默认的参数。使用 DPF-Series 设备时，可以直接调用这些默认的参数，也可以自己新建参数。

15.2 范例：本地数据库认证

在本例中，采用本地数据库对用户进行认证。 将定义名为 auth_grp 和 static_grp 的本地用户组。然后创建三个 auth 用户 darry、linda 和 lara 关联 auth_grp。再定义一个名为 mary 的静态用户（IP：1.2.2.50，MAC：00-00-ab-cd-12-34）关联 static_grp。策略中规定地址为 1.2.2.5～1.2.2.50 的用户访问 HTTP 服务需要进行 Web 认证，其它服务不需要认证。



CLI

1. 接口

```
set vif vif1 zone l3-in
set vif vif3 zone l3-out
set vif vif1 web-auth enable
set vif vif1 ip 1.2.2.1 netmask 255.255.255.0
```

set vif vif3 ip 1.1.1.1 netmask 255.255.255.0
set vif vif1 filters enable web,telnet,ping
set vif vif3 filters enable web,telnet,ping

2. 路由

set route ip 0.0.0.0 0.0.0.0 1.1.1.250

3. 用户组

eum set group auth_grp authentication web_8021x authorization normal accounting noaccounting
eum set group static_grp authentication web_8021x authorization normal accounting noaccounting

4. 用户

eum set subscriber auth name darry group auth_grp password darry123
eum set subscriber auth name linda group auth_grp password linda123
eum set subscriber auth name lara group auth_grp password lara123
eum set subscriber static name mary ip 1.2.2.50 mac 00-00-ab-cd-12-34 group static_grp

5. 策略

firewall set policy from ANY to ANY src-addr 1.2.2.5-1.2.2.50 dst-addr ANY service DNS action permit status enable
firewall set policy from ANY to ANY src-addr 1.2.2.5-1.2.2.50 dst-addr ANY service HTTP action auth auth-server-type default status enable
firewall set policy from ANY to ANY src-addr ANY dst-addr ANY service ANY action permit status enable

WEB 配置

WEB 的配置与 CLI 的配置相对应：

1. 接口

进入 **网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)->Vif1**，修改 zone 为 l3-in，启用“web 认证”，提交之后再点击按钮“**Set VIF IP**”添加 IP 地址 1.2.2.1/24。

修改虚拟接口 提交 取消 返回

虚接口名称	vif1	物理口/汇聚接口	lan1	有效	○ 是 ⊙ 否
VLAN	1	区域	l3-in		
加VLAN标签	☐	工作模式	路由模式		
地址转换	☐ 启用				
报文允许	☑ web ☑ telnet ☐ ssh ☑ ping ☐ snmp ☐ 全选				
认证开关	☑ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

图102.　　接口1

同理修改虚拟接口 vif3 的 zone 为 l3-out，配置 IP 地址为 1.1.1.1/24，如下图所示：

虚拟接口 新增

序号	名称	物理接口/汇聚口	VLAN	IP地址1/掩码	工作模式	区域	有效	操作
共 9 条记录 当前第 1 页								
1	vif0	lan0	1		透明模式	l2-in	是	
2	vif1	lan1	1		路由模式	l3-in	否	
3	vif2	lan2	1		路由模式	office	否	
4	vif3	lan3	1		路由模式	l3-out	否	
5	vif4	lan4	1		透明模式	l2-in	是	
6	vif5	lan5	1		透明模式	l2-in	是	
7	vif6	lan6	1		透明模式	l2-in	是	
8	vif7	lan7	1		透明模式	l2-in	是	
9	vif9	wan0	1		透明模式	l2-in	是	

图103.　　接口2

2. 路由

进入 **网络配置(NETWORK)->路由配置(Routing)->网络路由(Static Routing)->新增(CreateNew)**，添加一条到 1.1.1.250 的默认路由：

新增网络路由表			提交 取消 返回
IP地址	0.0.0.0	子网掩码	0.0.0.0
网关/ISP	1.1.1.250		
*IP地址 0.0.0.0 掩码 0.0.0.0 代表缺省路由			

图104. 路由

3. 用户组

分别为动态认证用户和静态认证用户建立两个用户组 auth_grp 和 static_grp。

进入 **USER-> Group Info->User Group->新增(CreateNew)**，配置一个认证用户组：

新增用户组			提交 取消 返回
名称	auth_grp		
注释			
认证策略	web_8021x	授权策略	normal
计费策略	noaccounting	黑名单控制	
强制重新认证	○ 启用 ⦿ 禁用		
最大认证次数	1	超出后动作	本次失败

图105. 认证用户组

建一个静态用户组：

新增用户组			提交 取消 返回
名称	static_grp		
注释			
认证策略	web_8021x	授权策略	normal
计费策略	noaccounting	黑名单控制	
强制重新认证	○ 启用 ⦿ 禁用		
最大认证次数	1	超出后动作	本次失败

图106. 静态用户组

4. 用户

进入 **USER->Users-> Auth Users**，建立认证用户需要用户名、密码和组三个要素。如果不输入密码，系统将启用默认的密码（即，用户名＋a1*）

新增认证用户			提交 取消 返回
名称	darry		
注释			
组	aurth_grp	☑ 显示高级	
密码			
重复密码			
IP地址	0.0.0.0		
MAC地址	00 - 00 - 00 - 00 - 00 - 00		
VLAN		端口号	
是否锁定	unlock	主机名	
黑名单控制	⦿ 启用 ○ 禁用		
IKE ID			

图107. **认证用户**

同理建立了三个认证用户，darry 、lara 和 linda，都属于 auth_grp 组

添加静态用户，默认不用设置高级菜单里的选项。而用户名、组、MAC 和 IP 地址四个要素

是必须的。建立一个名为 mary 的静态用户，如下图所示：

新增静态用户		提交 取消 返回
名称	marry	
注释		
IP地址	1.2.2.50	
MAC地址	00 - 00 - ab - cd - 12 - 34	
组	static_grp	☐ 显示高级

图108.　　静态用户

5. 策略

当需要认证时，必须首先要配置一条允许 DNS 服务的策略，这样才能弹出认证窗口；然后再配置一条动作是“auth”的策略来启用认证功能，最后配置一条允许用户信息流通过的策略，具体配置如下所示。

进入**安全(SECURITY)-> 安全策略(Policies)->新增(Create New)**，配置第一条允许 DNS 的全局策略：

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 [ ] 之前 ⦿ 最后		
安全区			
源安全区	ANY	目的安全区	ANY
地址/用户/地址簿			
	⦿ 源 地址 ○ 用户 ○ 地址簿	1.2.2.5-1.2.2.50	
	⦿ 目的地址 ○ 用户 ○ 地址簿		
动作	PERMIT	服务	DNS
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☐ 显示高级	

图109.　　策略

然后配置认证策略，选择本地数据库认证。如下：

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 [ ] 之前 ⦿ 最后		
安全区			
源安全区	ANY	目的安全区	ANY
地址/用户/地址簿			
	⦿ 源 地址 ○ 用户 ○ 地址簿	1.2.2.5-1.2.2.50	
	⦿ 目的地址 ○ 用户 ○ 地址簿		
动作	AUTH	服务	HTTP
认证	○ 缺省认证服务器 ⦿ 本地 ○ RADIUS ○ LDAP ○ POP3 ○ AD		
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☐ 显示高级	

图110.　　策略

最后配置允许用户信息流通过的策略：

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 [ ] 之前 ⦿ 最后		
安全区			
源安全区	ANY	目的安全区	ANY
地址/用户/地址簿			
	⦿ 源 地址 ○ 用户 ○ 地址簿		
	⦿ 目的地址 ○ 用户 ○ 地址簿		
动作	PERMIT	服务	ANY
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☐ 显示高级	

图111.　　策略

添加完成后，在‘策略列表’里选择 all 可以看到刚才添加的策略，默认系统是显示全局策略：

策略列表: All

新增 ☐ 全选 提交

序号	源地址/用户/地址簿	目的地址/用户/地址簿	定时计划	安全配置	服务	匹配计数	动作	状态	操作
eng -> l3-out 共 1 条记录									
1	ANY	ANY			ANY	0	permit	☑	
office -> l3-out 共 1 条记录									
1	ANY	ANY			ANY	0	permit	☑	
l3-in -> l3-out 共 1 条记录									
1	ANY	ANY			HTTP	0	pat	☑	
全局 共 3 条记录									
1	ANY	ANY			ANY	0	permit	☑	
2	1.2.2.7-1.2.2.126	ANY			FTP	0	deny	☑	
3	1.2.2.5-1.2.2.50	ANY			HTTP	0	auth	☑	

图112. 策略

15.3 设备认证

DPF-Series 设备支持对用户进行设备认证。接口上启用了设备认证，那么用户认证时，就会比较此用户的主机名和 MAC 地址是否存在“设备认证”配置中，如果没有就不允许此用户认证，就连认证窗口都不能弹出。这个功能可以限制接入网络的设备。也就是说，没有定义的设备不能访问网络。

在 **13.2 节“范例：本地数据库认证”**中，再启用设备认证，其它完全相同。这就需要在 vif1 上启用设备认证，并添加“设备认证”的相关配置。为简单起见，这里只列出需要添加的配置，其它相同的不再说明。

CLI

1. 启用设备认证

   set vif vif1 device-auth enable

2. 配置设备认证

   eum set device-auth lara mac 00-ab-cd-01-02-06 hostname LARA group hardware
   eum set device-auth linda mac 00-ab-cd-01-02-05 hostname LINDA group hr
   eum set device-auth marry mac 00-00-ab-cd-12-34 hostname MARRY group office
   eum set device-auth darry mac 00-ab-cd-01-02-03 hostname DARRY group software

WEB 配置

WEB的配置与CLI的配置相对应。

1. 启用设备认证

   进入 **网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)->Vif1**，在 vif1 上启用‘Device Auth’(粉色框所示)：

修改虚拟接口 提交 取消 返回

虚接口名称	vif1	物理口/汇聚接口	lan1	有效	○ 是 ⊙ 否
VLAN	1	区域	l3-in		
加VLAN标签	☐	工作模式	路由模式		
地址转换	☐ 启用				
报文允许	☑ web ☑ telnet ☐ ssh ☑ ping ☐ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

图113. vif设置

2. 配置设备认证

   进入 **USER->Users-> Device Auth**，配置设备认证参数。这里的 Group (和 Name) 与用户的

用户组(和用户名)没有直接的关系，可以根据管理员的需要进行定义。例如，为主机 LARA 配置设备认证：

新增设备 认证策略	提交 取消 返回
名称	lara
设备名	LARA
设备MAC	00 - AB - CA - 01 - 02 - 06
设备组	hardware

图114. 设备认证

定义了四个主机的设备认证参数，如下：

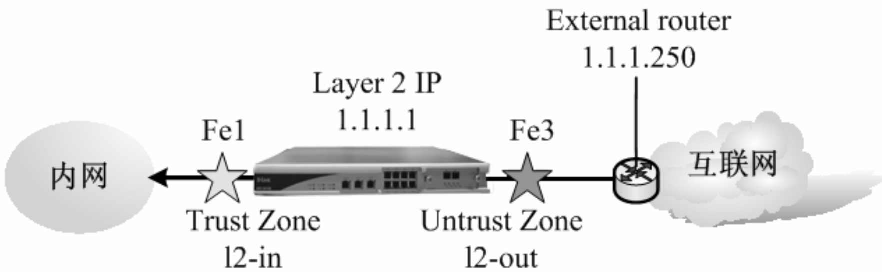
设备认证 新增

序号	名称	设备名	MAC	设备组	操作
1	lara	LARA	00-AB-CA-01-02-06	hardware	
2	linda	LINDA	00-AB-CD-01-02-05	hr	
3	marry	MARRY	00-00-AB-CD-12-34	office	
4	darry	DARRY	00-AB-CD-01-02-03	sofeware	

图115. 查看设备认证

15.4 范例: POP3 服务器认证

在本例中，采用 POP3 服务器对用户进行 WEB 认证。几乎所有的内网都有邮箱帐号，为了简化管理员对帐号的管理，不需要再单独维护一套认证用户的帐号，可以采用现有的 POP3 帐号对用户进行认证。在配置认证策略的时候，只需要将认证服务器指向 POP3 服务器即可，不需要再单独定义认证用户。既简化了对帐号的管理，又简化了对认证用户的配置。



定义名为 ourpop3 的 POP3 服务器，配置好 POP3 服务器后，就会在 DPF-Series 设备上自动生成一个 POP3 用户组。本例中自动生成的组名为 pop3-ourpop3-group。策略中规定内网所有的用户访问外网时需要认证，DPF-Series 设备工作于透明模式。

另外，在执行 POP3 认证的时候，DPF-Series 设备需要和 POP3 服务器建立连接，从而交换用户名和密码等，所以 DPF-Series 设备必须有一条到 POP3 服务器的主动路由。本例中，DPF-Series 设备工作于透明模式，为此，需要先添加一个 Layer 2 IP，再添加一条默认路由。

CLI

1. 接口

```
set vif vif1 zone l2-in
set vif vif3 zone l2-out
set vif vif1 web-auth enable
set vif vif1 filters enable web,telnet,ping
set vif vif3 filters enable web,telnet,ping
```

2. Layer 2 IP

```
set l2-if ip 1.1.1.1 netmask 255.255.255.0
```

3. 路由

   set route ip 0.0.0.0 0.0.0.0 1.1.1.250

4. RADIUS服务器

   eum set pop3 ourpop3 server mail.ourpop3.net timeout 30 default-group enable

5. 策略

   firewall set policy from l2-in to l2-out src-addr ANY dst-addr ANY service DNS action permit status enable

   firewall set policy from l2-in to l2-out src-addr ANY dst-addr ANY service ANY action auth auth-server-type pop3 auth-server ourpop3 status enable

   firewall set policy from l2-in to l2-out src-addr ANY dst-addr ANY service ANY action permit status enable

WEB 配置

WEB 配置与 CLI 的配置相对应：

1. 接口

   进入 **网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)->Vif1**，修改虚拟接口 vif3 的 zone 为 l2-out

修改虚拟接口					提交 取消 返回
虚接口名称	vif3	物理口/汇聚接口	lan3	有效	○ 是 ⊙ 否
VLAN	1	区域	l3-out		
加VLAN标签	☐	工作模式	路由模式		
地址转换	☐ 启用				
报文允许	☑ web ☑ telnet ☑ ssh ☑ ping ☐ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

图116. 接口

   进入 **网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)->Vif1**，启用 vif1 上的 web 认证开关

修改虚拟接口					提交 取消 返回
虚接口名称	vif1	物理口/汇聚接口	lan1	有效	○ 是 ⊙ 否
VLAN	1	区域	l2-in		
加VLAN标签	☐	工作模式	路由模式		
地址转换	☐ 启用				
报文允许	☑ web ☑ telnet ☐ ssh ☑ ping ☐ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

图117. 启用web认证

2. Layer 2 IP

   进入 **网络配置(NETWORK)->网络接口(Interfaces)->Layer 2**，配置一个二层 IP，用于建立到 POP3 服务器的路由

新增IP			提交 取消 返回
IP地址	1.1.1.1	子网掩码	255.255.255.0

图118. layer 2 IP

3. 路由

   进入 **网络配置(NETWORK)->路由配置(Routing)->网络路由(Static Routing)->新增(CreateNew)**，添加一条到 1.1.1.250 的默认路由：

新增网络路由表			提交 取消 返回
IP地址	0.0.0.0	子网掩码	0.0.0.0
网关/ISP	1.1.1.250		
*IP地址 0.0.0.0 掩码 0.0.0.0 代表缺省路由			

图119.　　路由

4. POP3 服务器

   要通过 POP3 服务器进行认证，则需要先建立一个 POP3 服务器。

   进入 **User->Authen-Servers->POP3 Server**，输入 POP3 服务器的网址或者 IP

新增 POP3 服务器			提交 取消 测试 返回
名称	ourpop3		
注释			
POP3服务器	mail.ourpop3.net	超时时间(秒)	30

图120.　　POP3 server

5. 策略

   当需要用户认证时，必须首先要配置一条允许 DNS 服务的策略，这样才能弹出认证窗口；然后再配置一条动作是“auth”的策略来启用认证功能，最后配置一条允许用户信息流通过的策略，具体配置如下所示。

   进入**安全(SECURITY)-> 安全策略(Policies)->新增(Create New)**，配置第一条允许 DNS 的全局策略：

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 ____ 之前 ⦿ 最后		
安全区			
源安全区	l2-in	目的安全区	l2-out
地址/用户/地址簿			
	⦿ 源 地址 ○ 用户 ○ 地址簿		
	⦿ 目的地址 ○ 用户 ○ 地址簿		
动作	PERMIT	服务	DNS
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☐ 显示高级	

图121.　　策略

然后配置认证策略，选择 POP3 认证(数据库选择 ourpop3)。如下：

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 ____ 之前 ⦿ 最后		
安全区			
源安全区	l2-in	目的安全区	l2-out
地址/用户/地址簿			
	⦿ 源 地址 ○ 用户 ○ 地址簿		
	⦿ 目的地址 ○ 用户 ○ 地址簿		
动作	AUTH	服务	ANY
认证	○ 缺省认证服务器 ○ 本地 ○ RADIUS ○ LDAP ⦿ POP3 ourpop3 ○ AD		
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☐ 显示高级	

图122.　　策略

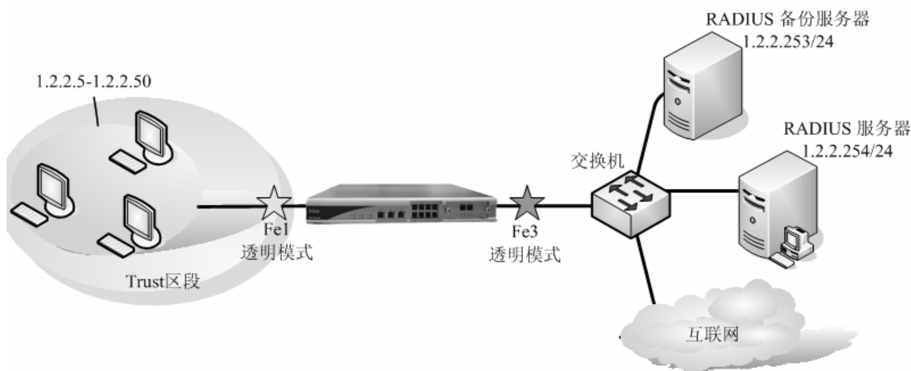
最后配置允许用户信息流通过的策略：

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 之前 ⦿ 最后		
安全区			
源安全区	l2-in	目的安全区	l2-out
地址/用户/地址簿			
	⦿ 源 地址 ○ 用户 ○ 地址簿		
	⦿ 目的地址 ○ 用户 ○ 地址簿		
动作	PERMIT	服务	ANY
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☐ 显示高级	

图123. 策略

15.5 范例: RADIUS AUTH 服务器认证

在本例中，采用 RADIUS Auth 服务器对用户 WEB 进行认证。定义名为 emily 的 RADIUS Auth 服务器，服务器的 IP 为 1.2.2.254，备份服务器的 IP 为 1.2.2.253。配置 RADIUS Auth 服务器时启用默认组，就会在 DPF-Series 设备上自动生成一个用户组，不用单独为 RADIUS auth 配置用户组。本例中自动生成的组名为 radius-emily-group。同时在 RADIUS Auth 服务器上定义 auth 用户和相关参数。策略中规定地址为 1.2.2.5～1.2.2.50 的用户访问 HTTP 服务需要进行 Web 认证，其它服务不需要认证。启用计费功能，计费服务器与认证服务器使用同一台机器。此例中，DPF-Series 设备工作于透明模式。



另外，在执行 Radius 认证的时候，DPF-Series 设备需要和 Radius 服务器建立连接，从而交换用户名等，所以 DPF-Series 设备必须有一条到 POP3 服务器的主动路由。由于此例中，DPF-Series 设备工作于透明模式，并且和 Radius 服务器是直连的，所以只需要添加一个同网段的 Layer 2 IP 即可。

CLI

1. 接口
```
set vif vif1 zone l2-in
set vif vif3 zone l2-out
set vif vif1 web-auth enable
set vif vif1 filters enable web,telnet,ping
set vif vif3 filters enable web,telnet,ping
```
2. Layer 2 IP
```
set l2-if ip 1.2.2.1 netmask 255.255.255.0
```
3. RADIUS服务器
```
eum set radius emily ip 1.2.2.254 auth-port 1812 acct-port 1813 key Dlink timeout 30 backup 1.2.2.253 default-group enable
```
4. 计费策略
```
eum set policy accounting raduis_account mode enable server emily interval 30
```

5. 修改用户组

   eum set group radius-emily-group authentication web_8021x authorization normal accounting raduis_account

6. 策略

   firewall set policy from ANY to ANY src-addr 1.2.2.5-1.2.2.50 dst-addr ANY service DNS action permit status enable

   firewall set policy from ANY to ANY src-addr 1.2.2.5-1.2.2.50 dst-addr ANY service HTTP action auth auth-server-type radius auth-server emily status enable

   firewall set policy from ANY to ANY src-addr ANY dst-addr ANY service ANY action permit status enable

WEB 配置

WEB 配置与 CLI 的配置相对应：

1. 接口

   进入 **网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)->Vif1**，修改虚拟接口 vif3 的 zone 为 l2-out

修改虚拟接口				提交 取消 返回	
虚接口名称	vif3	物理口/汇聚接口	lan3	有效	○ 是 ⊙ 否
VLAN	1	区域	l2-out		
加VLAN标签	☐	工作模式	路由模式		
地址转换	☐ 启用				
报文允许	☑ web ☑ telnet ☐ ssh ☑ ping ☐ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

图124. 接口

进入 **网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)->Vif1**，启用 vif1 上的 web 认证开关

修改虚拟接口				提交 取消 返回	
虚接口名称	vif1	物理口/汇聚接口	lan1	有效	○ 是 ⊙ 否
VLAN	1	区域	l2-in		
加VLAN标签	☐	工作模式	路由模式		
地址转换	☐ 启用				
报文允许	☐ web ☐ telnet ☐ ssh ☐ ping ☐ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

图125. 启用web认证

2. Layer 2 IP

   进入 **网络配置(NETWORK)->网络接口(Interfaces)->Layer 2**，配置一个二层 IP，用于建立到 Radius 服务器的通信

新增IP			提交 取消 返回
IP地址	1.2.2.1	子网掩码	255.255.255.0

图126. layer 2 IP

3. RADIUS 服务器

   要通过 RADIUS Auth 服务器进行认证，则需要先建立一个 RADIUS Auth 服务器。进入 **User->Authen-Servers->RADIUS Server**，其中 1.2.2.254 为主服务器，1.2.2.253 为备份服务器。

新增RADIUS 服务器		提交 取消 测试 返回	
名称	emily		
注释			
IP地址	1.2.2.254	备用IP地址	1.2.2.253
认证端口	1812	计费端口	1813
超时时间（秒）	30	密钥	
创建缺省组	☑		

4. 计费策略

进入 **USER->Group Info-> Accounting ->新增(Create New)**，增加一个计费策略，计费服务器选择emily。计费间隔默认是 30 秒，可以根据需要修改。

新增计费策略	提交 取消 返回
名称	radius-accout
注释	
计费模式	⦿ 启用 ○ 禁用
服务器	emily
间隔	30 (秒)

图127.　　计费策略

5. 修改用户组

进入 **USER->Group Info-> User Group**，修改 radius-emily-group

用户组　新增

序号	名称	认证策略	授权策略	计费策略	黑名单	强制重新认证	操作
共 5 条记录							
1	normal_group	web	normal	noaccounting		禁用	
2	priority_group	web	priority	noaccounting		禁用	
3	host_sec_fail	web	normal	noaccounting		禁用	
4	pop3-ourpop3-group	web	normal	noaccounting		禁用	
5	radius-emily-group	web	normal	noaccounting		禁用	

图128.　　修改用户组

修改组 radius-emily-group 的计费策略为 raduis_account

修改用户组		提交 取消 返回	
名称	radius-emily-group		
注释			
认证策略	web-8021x	授权策略	normal
计费策略	radius-accout	黑名单控制	
强制重新认证	○ 启用 ⦿ 禁用		
最大认证次数	1	超出后动作	本次失败

图129.　　修改用户组

6. 策略

当需要用户认证时，必须首先要配置一条允许 DNS 服务的策略，这样才能弹出认证窗口；然后再配置一条动作是“auth”的策略来启用认证功能，最后配置一条允许用户信息流通过的策略，具体配置如下所示。

进入**安全(SECURITY)-> 安全策略(Policies)->新增(Create New)**，配置第一条允许 DNS 的全局策略：

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 [ ] 之前 ⦿ 最后		
安全区			
源安全区	ANY	目的安全区	ANY
地址/用户/地址簿			
	⦿ 源 地址 ○ 用户 ○ 地址簿	1.2.2.5-1.2.2.50	
	⦿ 目的地址 ○ 用户 ○ 地址簿		
动作	PERMIT	服务	DNS
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☐ 显示高级	

图130. 策略

然后配置认证策略，选择 RADUIS 认证(数据库选择 emily)。如下：

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 [ ] 之前 ⦿ 最后		
安全区			
源安全区	ANY	目的安全区	ANY
地址/用户/地址簿			
	⦿ 源 地址 ○ 用户 ○ 地址簿	1.2.2.5-1.2.2.50	
	⦿ 目的地址 ○ 用户 ○ 地址簿		
动作	AUTH	服务	HTTP
认证	○ 缺省认证服务器 ○ 本地 ⦿ RADIUS emily ○ LDAP ○ POP3 ○ AD		
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☐ 显示高级	

图131. 策略

最后配置允许用户信息流通过的策略：

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 [ ] 之前 ⦿ 最后		
安全区			
源安全区	ANY	目的安全区	ANY
地址/用户/地址簿			
	⦿ 源 地址 ○ 用户 ○ 地址簿		
	⦿ 目的地址 ○ 用户 ○ 地址簿		
动作	PERMIT	服务	ANY
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☐ 显示高级	

图132. 策略

添加完成后，在‘策略列表’里选择 all 可以看到刚才添加的策略，默认系统是显示全局策略：

策略列表: All

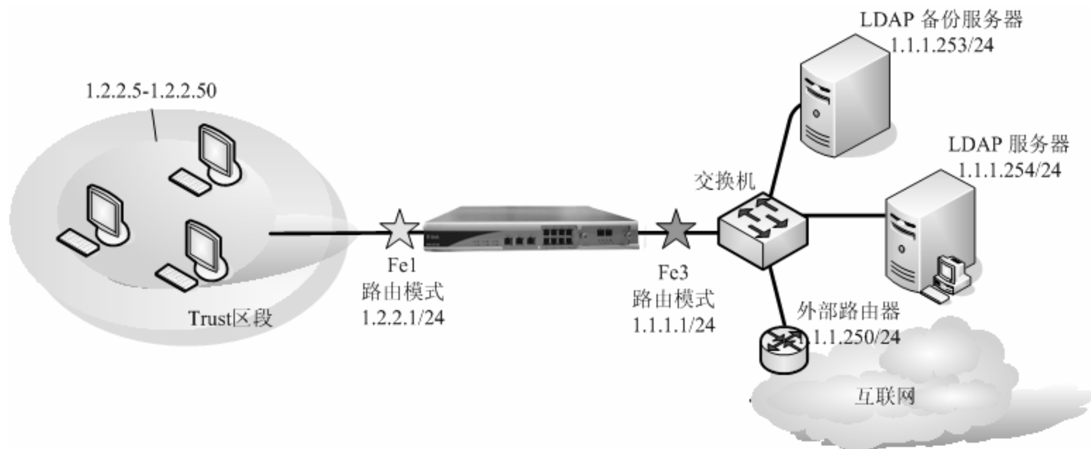
新增 ☐ 全选 提交

序号	源地址/用户/地址簿	目的地址/用户/地址簿	定时计划	安全配置	服务	匹配计数	动作	状态	操作
eng -> l3-out 共 1 条记录									
1	ANY	ANY			ANY	0	permit	☑	
office -> l3-out 共 1 条记录									
1	ANY	ANY			ANY	0	permit	☑	
l3-in -> l3-out 共 1 条记录									
1	ANY	ANY			HTTP	0	pat	☑	
l2-in -> l2-out 共 2 条记录									
1	ANY	ANY			DNS	0	permit	☑	
2	ANY	ANY			ANY	0	auth	☑	
全局 共 6 条记录									
1	ANY	ANY			ANY	0	permit	☑	
2	1.2.2.7-1.2.2.126	ANY			FTP	0	deny	☑	
3	1.2.2.5-1.2.2.50	ANY			HTTP	0	auth	☑	
4	ANY	ANY			HTTP	0	auth	☑	
5	1.2.2.5-1.2.2.50	ANY			DNS	0	permit	☑	
6	1.2.2.5-1.2.2.50	ANY			HTTP	0	auth	☑	

图133. 策略

15.6 范例: LDAP AUTH 服务器认证

在本例中，采用 LDAP Auth 服务器对用户进行认证。 定义名为 abcd 的 LDAP Auth 服务器，服务器的 IP 为 1.1.1.254，备份服务器的 IP 为 1.1.1.253。配置 LDAP Auth 服务器时启用默认组，就会在 DPF-Series 设备上自动生成一个用户组，不用单独为 LDAP auth 配置用户组。本例中自动生成的组名为 ldap-abcd-group。同时在 LDAP Auth 服务器上定义 auth 用户和相关参数。策略中规定地址为 1.2.2.5～1.2.2.50 的用户访问 HTTP 服务需要进行 802.1x 认证，其它服务不需要认证。本例中，DPF-Series 设备工作与路由模式，也可以工作与透明模式。



CLI

1. 接口

```
set vif vif1 zone l3-in
set vif vif6 8021x status enable
set vif vif3 zone l3-out
set vif vif1 filters enable web,telnet,ping
set vif vif3 filters enable web,telnet,ping
set vif vif1 ip 1.2.2.1 netmask 255.255.255.0
set vif vif3 ip 1.1.1.1 netmask 255.255.255.0
```

2. 路由

```
set route ip 0.0.0.0 0.0.0.0 1.1.1.250
```

3. LDAP服务器

```
eum set ldap abcd ip 1.1.1.254 port 389 cn "cn" dn "o=Dlink" timeout 30 backup 1.1.1.253 default-group enable
```

4. 策略

```
firewall set policy from ANY to ANY src-addr ANY dst-addr ANY service DNS action permit status enable
firewall set policy from ANY to ANY src-addr 1.2.2.5-1.2.2.50 dst-addr ANY service HTTP action auth auth-server-type ldap auth-server abcd status enable
firewall set policy from ANY to ANY src-addr ANY dst-addr ANY service ANY action permit status enable
```

WEB 配置

WEB 配置与 CLI 的配置相对应：

1. 接口

进入 **网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)->Vif1**，修改 zone 为 l3-in，启用 “802.1x 认证”，提交之后再点击按钮“**Set VIF IP**”添加 IP 地址 1.2.2.1/24。

修改虚拟接口 提交 取消 返回

虚接口名称	vif1	物理口/汇聚接口	lan1	有效	○ 是 ⊙ 否
VLAN	1	区域	l3-in		
加VLAN标签	☐	工作模式	路由模式		
地址转换	☐ 启用				
报文允许	☐ web ☐ telnet ☐ ssh ☐ ping ☐ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

图134.　　接口1

2. 路由

进入 **网络配置(NETWORK)->路由配置(Routing)->网络路由(Static Routing)->新增(CreateNew)**，添加一条到 1.1.1.250 的默认路由：

新增网络路由表 提交 取消 返回

IP地址	0.0.0.0	子网掩码	0.0.0.0
网关/ISP	1.1.1.250		
*IP地址 0.0.0.0 掩码 0.0.0.0 代表缺省路由			

图135.　　路由

3. LDAP 服务器

要通过 LDAP Auth 服务器进行认证，则需要先建立一个 LDAP Auth 服务器。进入 **User->Authen-Servers->LDAP Server**, 其中 1.1.1.254 为主服务器，1.1.1.253 为备份服务器。

新增LDAP 服务器 提交 取消 测试 返回

名称	abcd		
注释			
IP地址	1.1.1.254	备用IP地址	1.1.1.253
认证端口	389	超时时间（秒）	30
cn	cn	dn	c=acenet
创建缺省组	☑		

图136.　　ldap server

4. 策略

当需要用户认证时，必须首先要配置一条允许 DNS 服务的策略，这样才能弹出认证窗口；然后再配置一条动作是“auth”的策略来启用认证功能，最后配置一条允许用户信息流通过的策略，具体配置如下所示。

进入**安全(SECURITY)-> 安全策略(Policies)->新增(Create New)**，配置第一条允许 DNS 的全局策略：

新增安全策略 提交 取消 返回

位置	○ 置顶 ○ 在 ＿ 之前 ⊙ 最后		
安全区			
源安全区	ANY	目的安全区	ANY
地址/用户/地址簿			
	⊙ 源 地址 ○ 用户 ○ 地址簿	1.2.2.5-1.2.2.50	
	⊙ 目的地址 ○ 用户 ○ 地址簿		
动作	PERMIT	服务	DNS
日志	☐ log		
防病毒	☐ 防病毒		
使能	⊙ 启用 ○ 禁用	☐ 显示高级	

图137.　　策略

然后配置认证策略，选择 LDAP 认证(数据库选择 abcd)。如下：

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在	之前 ⦿ 最后	
安全区			
源安全区	ANY	目的安全区	ANY
地址/用户/地址簿			
	⦿ 源 地址 ○ 用户 ○ 地址簿	1.2.2.5-1.2.2.50	
	⦿ 目的地址 ○ 用户 ○ 地址簿		
动作	AUTH	服务	HTTP
认证	○ 缺省认证服务器 ○ 本地 ○ RADIUS ⦿ LDAP abcd ○ POP3 ○ AD		
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☐ 显示高级	

图138.　　策略

最后配置允许用户信息流通过的策略：

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在	之前 ⦿ 最后	
安全区			
源安全区	ANY	目的安全区	ANY
地址/用户/地址簿			
	⦿ 源 地址 ○ 用户 ○ 地址簿		
	⦿ 目的地址 ○ 用户 ○ 地址簿		
动作	PERMIT	服务	ANY
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☐ 显示高级	

图139.　　策略

策略列表: All

新增　☐ 全选 提交

序号	源地址/用户/地址簿	目的地址/用户/地址簿	定时计划	安全配置	服务	匹配计数	动作	状态	操作
eng -> l3-out 共 1 条记录									
1	ANY	ANY			ANY	0	permit	☑	
office -> l3-out 共 1 条记录									
1	ANY	ANY			ANY	0	permit	☑	
l3-in -> l3-out 共 1 条记录									
1	ANY	ANY			HTTP	0	pat	☑	
l2-in -> l2-out 共 2 条记录									
1	ANY	ANY			DNS	0	permit	☑	
2	ANY	ANY			ANY	0	auth	☑	
全局 共 9 条记录									
1	ANY	ANY			ANY	0	permit	☑	
2	1.2.2.7-1.2.2.126	ANY			FTP	0	deny	☑	
3	1.2.2.5-1.2.2.50	ANY			HTTP	0	auth	☑	
4	ANY	ANY			HTTP	0	auth	☑	
5	1.2.2.5-1.2.2.50	ANY			DNS	0	permit	☑	
6	1.2.2.5-1.2.2.50	ANY			HTTP	0	auth	☑	
7	1.2.2.5-1.2.2.50	ANY			DNS	0	permit	☑	
8	1.2.2.5-1.2.2.50	ANY			HTTP	0	auth	☑	
9	ANY	ANY			ANY	0	permit	☑	

添加完成后，在‘策略列表’里选择 all 可以看到刚才添加的策略，默认系统是显示全局策略：

图140.　　策略

15.7　黑名单

为了防止网络资源的滥用和方便管理员管理用户，DPF-Series 设备支持将用户加入黑名单的功能。对进入黑名单的用户可以采取惩罚机制，惩罚期限到了之后，该用户又可以正常使用网络。灵活的黑名单功能可以帮助管理员快速、准确的定位出谁肆意占有网络资源。黑名单可以基于以下三种来控制：

◆　Session：控制用户滥用 p2p、防止病毒等

◆ 流量：可控制用户总的流量的使用，防止用户肆意占用带宽
◆ 速率：可以防止蠕虫等病毒的突发性、或者防止某个时段某个用户占有大量带宽
一旦进入黑名单，当再次上网时，网页回弹出已经进入黑名单、是什么原因进入黑名单的。

使用黑名单功能的步骤如下：

1. 配置黑名单

首先输入黑名单的名称(这里为 auth_black)，可以配置每分钟、每日、每周、每月、每季度和每年需要限制的流量。然后配置当此用户进入黑名单后被惩罚的时间和类型，惩罚时间可以按天和分钟来计算，惩罚类型可以是让用户下线或者是修改其服务质量(包括上行和下行服务质量)。

进入 **USER>Blacklist ->Blacklist Config**，配置黑名单参数。这里配置的惩罚时间是 60 分钟，惩罚的类型是将用户的上行 QoS 修改为 100K、下行 QoS 修改为 200K。如下：

设置流量限制			提交 取消 返回
名称	auth_black		
每日流量限制 (KByte)	发送: 1000	接收: 1500	总流量: 0
每周流量限制 (KByte)	发送: 5000000	接收: 51000000	总流量: 0
每月流量限制 (KByte)	发送: 30000000	接收: 310000000	总流量: 0
每季度流量限制 (KByte)	发送: 1100000000	接收: 1200000000	总流量: 0
每年流量限制 (KByte)	发送: 4000000000	接收: 4100000000	总流量: 0
平均session数	在过去 15 分钟		
惩罚时间	60 ○天 ⊙分钟		
惩罚类型	○下线 ⊙修改服务质量 ○修改session数		
上行服务质量	100k	下行服务质量	200k

图141. 配置黑名单参数

2. 引用黑名单

在用户组里引用黑名单配置，这将使得这个组里的所有用户都使用这个黑名单的配置。如下为认证用户配置一个用户组，组名为 auth_grp，然后引用名为 auth_black 的黑名单配置。所有属于 auth_grp 组的用户都启用 auth_black 的黑名单配置。

进入 **USER-> Group Info->User Group->新增(CreateNew)**，如下：

新增用户组			提交 取消 返回
名称	auth_grp		
注释	the group for auth user		
认证策略	web-8021x	授权策略	normal
计费策略	noaccounting	黑名单控制	auth_black
强制重新认证	○启用 ⊙禁用		
最大认证次数		超出后动作	本次失败

图142. 新建用户组

用户组里引用了黑名单配置，但是某个用户可以启用或者禁用黑名单控制。例如，用户 linda 所在的用户组 auth_grp 引用了黑名单 auth_black 配置，但是 linda 可以禁用黑名单控制，而用户组 auth_grp 中其它用户仍然启用了黑名单控制。配置如下：

新增认证用户			提交 取消 返回
名称	linda		
注释			
组	auth_grop	☑ 显示高级	
密码			
重复密码			
IP地址	0.0.0.0		
MAC地址	00 - 00 - 00 - 00 - 00 - 00		
VLAN		端口号	
是否锁定	unlock	主机名	
黑名单控制	○ 启用 ⦿ 禁用		
IKE ID			

图143.　　引用黑名单配置

3.　查询黑名单用户

进入 **USER>Blacklist->Blacklist User**，可以查询到当前进入黑名单的所有用户的信息。

序号	用户名/IP	黑名单名	时间	动作	原因	门限值(KByte)	流量(KByte)
当前第 1 页							

图144.　　查询黑名单用户

4.　黑名单日志

可以输入想要查询的用户名/IP 地址、引用的黑名单名称、时间范围、进入黑名单的原因，以及进/出黑名单等参数来过滤黑名单 Log。不输入任何参数就是查询所有的黑名单 Log。

进入 **USER>Blacklist->Blacklist Log**，输入过滤参数。如下：

黑名单日志			查询 取消 清除
过滤条件			
用户名/IP		黑名单名	
开始时间		结束时间	
原因		动作	

图145.　　黑名单日志过滤条件

然后点击"**Query**"，查询结果如下：

序号	用户名/IP	黑名单名	时间	动作	原因	门限值(KByte)	流量(KByte)
当前第 1 页							

图146.　　黑名单查询结果

16 流量控制

16.1 简介

AG-Series 设备能够以每 IP（IP 段）、每用户、每会话、每时间段或每应用为基础保护、调整及提供带宽能力。每个流量分类都对应一个特定带宽分配策略，确保了每个流量类型都可获得适量的带宽。同时可以针对流量分类限制并发会话数、新建会话速率。可以阻止或限制在为普通 DoS 目标保留的端口中的流量。

AG-Series 设备支持两种方式的流量控制：

- ◆ 基于用户：基于用户的 QoS 是针对每个用户来进行带宽限制的。例如：某个授权策略里引用上行和下行都是 1M 的 QoS，那么所有引用这个授权策略的用户最大有 1M 的带宽。
- ◆ 基于策略： 基于策略的 QoS 是指所有符合这条策略的流都采用 QoS 指定的带宽。

基于用户的流量控制，通过对用户授权来控制用户以多大上行和下行带宽来访问网络。基于策略的流量控制，在策略中引用 QoS，可以指定每类信息流的带宽数量。如果基于用户和基于策略的 QoS 配置重叠时，以其中带宽小的为准。策略中Qos又分为两种类型：普通带宽控制和通道带宽。每种类型都可以进行以下三种流量控制：

- ✧ 总的带宽(Bidirection QoS)：上下行双向带宽总和
- ✧ 上行带宽(Up QoS)：上行带宽数量
- ✧ 下行带宽(Down QoS)：下行带宽数量

16.2 基于策略的 QOS

基于策略的 QoS 又分为两种：普通带宽酷虐固执和通道带宽控制。

普通带宽控制：

普通带宽控制可以对上行流量、下行流量和总的流量进行最大流量控制。普通带宽配置界面如下图：

Edit QoS	提交 取消 返回		
名称	normal-qos		
注释			
优先级	0 (7最高,0最低)	类型	带宽限制
发送(Kbits/s)	最大: 1000		
接收(Kbits/s)	最大: 2000		
总共(Kbits/s)	最大: 2500		
群组共享	☑		

图147. 普通带宽配置

参数说明：

- ◆ Priority：Qos优先级，0为最低级，7为最高优先级
- ◆ Send：上行流量最大值，单位为每秒1千位流
- ◆ Recv：下行流量最大值
- ◆ Total：上下行双向流量总和的最大值

例如：配置 qos1 上行流量为 1000Kbits/s，下行流量为 1500Kbits/s，总的流量为 2000Kbits/s:，则采用这条 Qos 的流的所有上行流量最大可有 1000Kbits/s 带宽，下行流量最大有 1500Kbits/s 带宽，总的上下行流量带宽不能超过 2000Kbits/s

通道带宽控制

通道带宽提供了更灵活的带宽控制方式，可以将带宽控制划分为若干个子带宽进行管理，每个子带宽都可以包含以下三种带宽配置。

✧ 最小带宽

  最小带宽特点是保证即使在网络繁忙时候，指定信息流也能够保证指定的最小带宽；在网络空闲时可以拥有超过指定最小带宽的带宽。但是，当没有指定信息流时，指定的最小带宽部分也不能被其他信息流使用。

✧ 最大带宽

  信息流所能拥有的最大带宽。

✧ 保障带宽

  使用保障带宽，即使在网络繁忙时候，也可以保证指定信息流的通畅；当没有指定信息流使用该保障带宽时，其他类型信息流可以使用这部分带宽。

  如 WEB 的最小带宽配置为 100K、保障带宽配置为 2M、最大带宽配置为 10M。不论网络中有无 WEB 流量，都会为 WEB 服务预留 100K 带宽，即这 100K 都不能被其它服务占用；当网络拥塞时可以给 WEB 服务保证 2M 的带宽；当网络空闲时，WEB 服务最大可以使用 10M 的带宽；当 WEB 服务流量很小时，其它流量可以租用 WEB 带宽。

每类带宽配置都包括上行、下行和总带宽流量控制。

配置通道带宽成功后，系统会自动生成一个 other 的子带宽配置项。Other 子带宽的默认值为：所有最小带宽为 0，最大带宽使用通道带宽的最大带宽值，所有保障带宽为 0。

通道带宽主带宽配置界面如下图：

新增服务质量　　提交　取消　返回

名称	tunnel-qos		
注释			
优先级	0 (7最高,0最低)	类型	通道带宽
发送(Kbits/s)	最大: 1000		
接收(Kbits/s)	最大: 2000		
总共(Kbits/s)	最大: 2500		

图148.　　通道带宽配置

通道带宽配置成功后返回 Qos 主页面，如下图：

服务质量　　新增

名称	优先级	发/收/总带宽(Kbits/s)	类型	操作
共 3 条记录				
normal-qos	0	max:1000KB/2.0MB/2.4MB	群组共享	
tunnel-qos	0	max:1000KB/2.0MB/2.4MB	通道带宽	

图149.　　Qos主页面

每个通道带都默认有一个 others 子带宽，点击通道带宽名称左边的▶可以看到默认自带宽如下图：

服务质量　　新增

名称	优先级	发/收/总带宽(Kbits/s)	类型	操作
共 3 条记录				
normal-qos	0	max:1000KB/2.0MB/2.4MB	群組共享	
tunnel-qos	0	max:1000KB/2.0MB/2.4MB	通道带宽	
tunnel-qos_others	0	guarantee:0KB/0KB/0KB	子带宽	

图150.　　Qos主页面

可以点击“操作”中的为通道带宽添加新的子带宽。子带宽配置界面如下图：

新增子带宽	提交 取消 返回		
名称	tunnel-qos-web		
注释			
优先级	1 (7最高,0最低)		
发送(Kbits/s)	最小: 0	最大: 1000	保障: 200
接收(Kbits/s)	最小: 0	最大: 2000	保障: 300
总共(Kbits/s)	最小: 0	最大: 2500	保障: 400

图151.　　子带宽配置

参数配置说明：

Name：子带宽名称

Priority：子带宽优先级。

Send， Rece， Total 为上行、下行和总带宽，分别都包含以下三种配置：

　　Min：最小带宽，默认为 0

　　Max：最大带宽，默认为主带宽的最大带宽值

　　Guarantee：保障带宽，默认为 0

如果某种带宽配置为 0 则表示不进行限制。

每个子带宽的最大带宽值都不能大于主带宽的最大带宽值。

策略中引用 Qos

配置 Qos

Edit QoS	提交 取消 返回		
名称	normal-qos		
注释			
优先级	0 (7最高,0最低)	类型	带宽限制
发送(Kbits/s)	最大: 1000		
接收(Kbits/s)	最大: 2000		
总共(Kbits/s)	最大: 2500		
群组共享	☑		

图152.　　配置moral-qos

在策略中引用 normal-qos

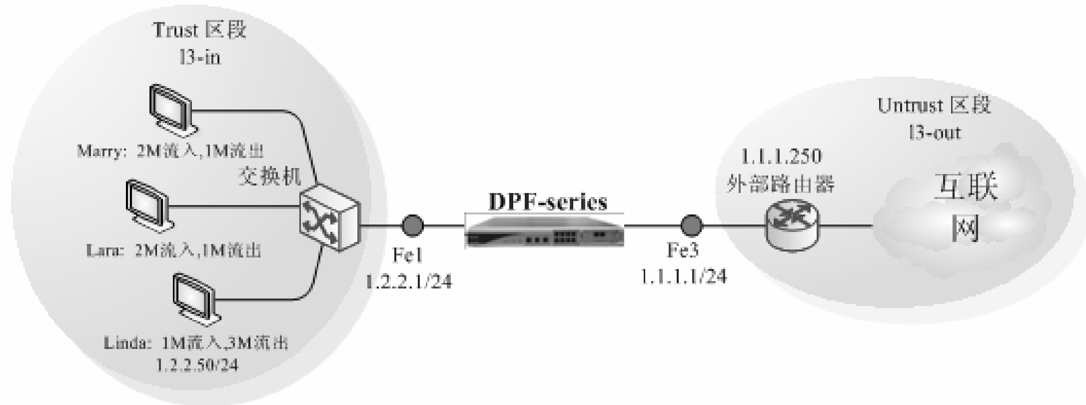
新增安全策略	提交 取消 返回		
位置	○ 置顶 ○ 在 之前 ◉ 最后		
安全区			
源安全区	ANY	目的安全区	ANY
地址/用户/地址簿			
	◉ 源 地址 ○ 用户 ○ 地址簿		
	◉ 目的地址 ○ 用户 ○ 地址簿		
动作	PERMIT	服务	ANY
日志	☐ log		
使能	◉ 启用 ○ 禁用	☑ 显示高级	
组			
源组		目的组	
定时计划		安全配置	
总服务质量	normal-qos		
监控	☐ 源 ☐ 目的	监控当前连接	☐
流量统计	☐		
注释			

图153.　　策略中引用normal-qos

以上配置得到的控制结果是：匹配策略的所有流访问网络的上行带宽不能超过 1000Kbits/s、下行带宽不能超过 2000Kbits/s，但总的流量却又不能超过 2500Kbits/s。

16.3 范例：基于用户的 QOS

本例中，有三个用户：Marry、Lara 和 Linda。其中 Marry 和 Lara 为认证用户，Linda 为静态用户。给 Marry 和 Lara 分配 2M 的下行带宽、1M 的上行带宽，给 Linda 分配 1M 的下行带宽、3M 的上行带宽。



系统默认有一个 1M 的 QoS，再定义一个 2M 和 3M 的 QoS，分别命名为 2M 和 3M。然后定义两个授权策略 auth 和 static，auth 下行 QoS 引用 2M，上行 QoS 引用 1M，static 下行 QoS 引用 1M，上行 QoS 引用 3M。最后定义两个认证用户 Marry 和 Lara，一个静态用户 Linda。Marry 和 Lara 所在的用户组(auth_grp)引用名为 auth 的授权策略，Linda 所在的用户组(static_grp)引用名为 static 的授权策略。

CLI

1. 接口

   set vif vif1 zone l3-in
   set vif vif3 zone l3-out
   set vif vif1 web-auth enable
   set vif vif1 ip 1.2.2.1 netmask 255.255.255.0
   set vif vif3 ip 1.1.1.1 netmask 255.255.255.0
   set vif vif1 filters enable web,telnet,ping
   set vif vif3 filters enable web,telnet,ping

2. 路由

   set route ip 0.0.0.0 0.0.0.0 1.1.1.250

3. 授权策略

   eum set policy authorization auth up-bandwidth 1000 down-bandwidth 2000 maxsrcsession 10 maxdestsession 10
   eum set policy authorization static up-bandwidth 3000 down-bandwidth 1000 maxsrcsession 10 maxdestsession 10

4. 用户组

   eum set group auth_grp authentication web_8021x authorization auth accounting noaccounting
   eum set group static_grp authentication web_8021x authorization static accounting noaccounting

5. 用户

   eum set subscriber auth name darry group auth_grp password darry123
   eum set subscriber auth name lara group auth_grp password lara123
   eum set subscriber static name linda ip 1.2.2.50 mac 00-00-ab-cd-12-34 group static_grp

6. 策略

   firewall set policy from l3-in to l3-out src-addr ANY dst-addr ANY service DNS action permit status enable
   firewall set policy from l3-in to l3-out src-addr ANY dst-addr ANY service ANY action auth

auth-server-type default status enable
firewall set policy from l3-in to l3-out src-addr ANY dst-addr ANY service ANY action permit status enable

WEB 配置

WEB 的配置与 CLI 的配置相对应：

1. 接口

进入 **网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)->Vif1**，修改 zone 为 l3-in ，启用“**web 认证**”，提交之后再点击 “**Set VIF IP**”按钮，添加 IP 地址 1.2.2.1/24。

修改虚拟接口 提交 取消 返回

虚接口名称	vif1	物理口/汇聚接口	lan1	有效	○ 是 ⊙ 否
VLAN	1	区域	l3-in		
加VLAN标签	☐	工作模式	路由模式		
地址转换	☐ 启用				
报文允许	☐ web ☐ telnet ☐ ssh ☐ ping ☐ snmp ☐ 全选				
认证开关	☑ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

图154. 修改接口

修改虚拟接口 vif3 的 zone 为 l3-out，配置 IP 地址为 1.1.1.1/24，如下图所示：

虚拟接口 新增

序号	名称	物理接口/汇聚口	VLAN	IP地址1/掩码	工作模式	区域	有效	操作
共 9 条记录 当前第 1 页								
1	vif0	lan0	1		透明模式	l2-in	是	
2	vif1	lan1	1		路由模式	l3-in	否	
3	vif2	lan2	1		路由模式	office	否	
4	vif3	lan3	1		透明模式	l2-out	是	
5	vif4	lan4	1		透明模式	l2-in	是	
6	vif5	lan5	1		透明模式	l2-in	是	
7	vif6	lan6	1		透明模式	l2-in	是	
8	vif7	lan7	1		透明模式	l2-in	是	
9	vif9	wan0	1		透明模式	l2-in	是	

图155. 查看接口

2. 路由

进入 **网络配置(NETWORK)->路由配置(Routing)->Static Routing>新增(Create New)**，添加一条到 1.1.1.250 的默认路由：

新增网络路由表 提交 取消 返回

IP地址	0.0.0.0	子网掩码	0.0.0.0
网关/ISP	1.1.1.250		
*IP地址 0.0.0.0 掩码 0.0.0.0 代表缺省路由			

图156. 路由

3. 授权策略

进入 **USER->Group Info->Authorization->新增(Create New)**，创建两个策略 auth 和 static。

修改授权策略 提交 取消 返回

名称	auth		
注释			
上行带宽	1000 Kbits/s	下行带宽	2000 Kbits/s
源会话	10	目的会话	10
定时计划		超出计划设置	☐

图157. 创建授权策略

创建完成后，结果如下：

授权策略设置 新增

序号	名称	上行带宽 (Kbits/s)	下行带宽 (Kbits/s)	源会话	目的会话	操作
共 3 条记录						
1	normal	1000	1000	50	50	
2	priority	10000	10000	0	0	
3	auth	1000	2000	10	10	

图158. 查看授权策略

4. 用户组

分别为动态认证用户和静态认证用户建立两个用户组：auth_grp 和 static_grp。

进入 **USER-> Group Info->User Group->新增(Create New)**，配置一个认证用户组：

新增用户组 提交 取消 返回

名称	auth_grp		
注释			
认证策略	web-8021x	授权策略	normal
计费策略	noaccounting	黑名单控制	
强制重新认证	○ 启用 ⊙ 禁用		
最大认证次数		超出后动作	本次失败

图159. 认证用户

再一个静态用户组：

新增用户组 提交 取消 返回

名称	static_grp		
注释			
认证策略	web-8021x	授权策略	normal
计费策略	noaccounting	黑名单控制	
强制重新认证	○ 启用 ⊙ 禁用		
最大认证次数		超出后动作	本次失败

图160. 静态用户

5. 用户

建立认证用户需要用户名、密码和组三个要素。用户名和密码是要区分大小写的。

如果不输入密码，系统将启用默认的密码（即，用户名＋a1*）；如果要设置密码，就点击"**Advanced……**"按钮，如下：

新增认证用户 提交 取消 返回

名称	marry		
注释			
组	auth_grop	☑ 显示高级	
密码	•••••••••		
重复密码	•••••••••		
IP地址	0.0.0.0		
MAC地址	00 - 00 - 00 - 00 - 00 - 00		
VLAN		端口号	
是否锁定	unlock	主机名	
黑名单控制	⊙ 启用 ○ 禁用		
IKE ID			

图161. 认证用户

添加静态用户，默认不用设置高级菜单里的选项。而用户名、组、MAC 和 IP 地址四个要素是必须的。如下：

新增静态用户	提交 取消 返回	
名称	linda	
注释		
IP地址	1.2.2.50	
MAC地址	00 - 00 - 00 - 00 - 00 - 00	
组	static_grp	☐ 显示高级

图162.　　静态用户

6. 策略

   当需要用户认证时，必须首先要配置一条允许 **DNS** 服务的策略，这样才能弹出认证窗口；然后再配置一条动作是“**auth**”的策略来启用认证功能，最后配置一条允许用户信息流通过的策略，具体配置如下所示。

   进入**安全(SECURITY)->安全策略(Policies)->新增(Create New)**，依次配置以上三条的策略，区域选择“l3-in -> l3-out”。添加完成后，在‘策略列表’里选择 all 可以看到刚才添加的策略，默认系统是显示全局策略。

策略列表: All

新增　☐ 全选 提交　清空

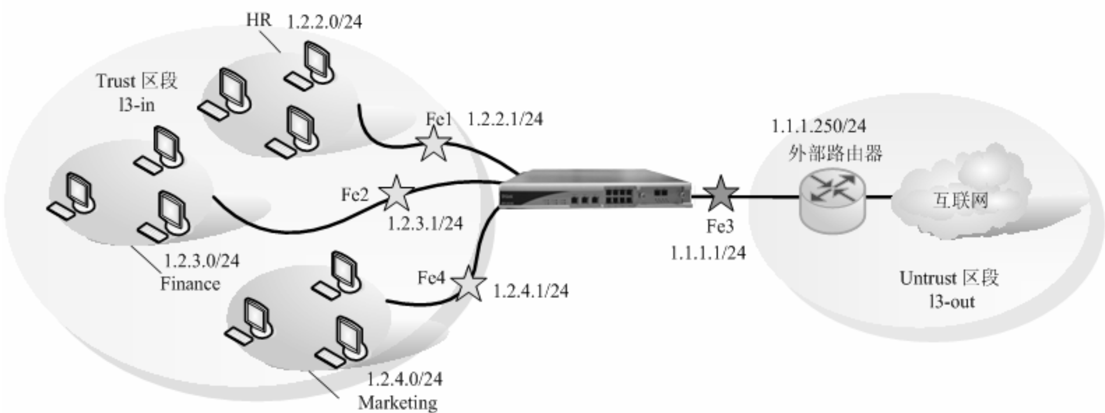
序号	源地址/用户/地址簿	目的地址/用户/地址簿	定时计划	安全配置	服务	匹配计数	动作	状态	操作
▼ l3-in -> l3-out 共 3 条记录									清除
1	ANY	ANY			DNS	0	permit	☑	
2	ANY	ANY			ANY	0	auth	☑	
3	ANY	ANY			ANY	0	permit	☑	
▼ 全局 共 0 条记录									清除

查看策略

16.4　范例：基于策略的普通带宽控制

某公司的市场部、财务部和人力资源三个部门都位于 Trust 区段 (l3-in)。定义这三个部门为：

- Marketing
- finance
- HR



要求实现以下流量控制:

- 三个部门之间的员工不能互访
- 市场部门的员工访问外网时上行带宽最大为 2M，下行带宽最大为 3M，但双向带宽总和不能超过 4M
- 人力资源部的员工访问外网时上行带宽限制为 1M，下行带宽限制为 2M
- 财务部的员工访问外网时上下行双向带宽总和不能超过 2M

系统默认定义了一个 1M 的 QoS 参数，再分别定义一个 2M、3M 和 4M 的 QoS 参数。人力资源的员工的 IP 地址为 1.2.2.0/24，财务部的员工的 IP 地址为 1.2.3.0/24，市场部的员工的 IP 地址为 1.2.4.0/24。

CLI

1. 接口

```
set vif vif1 zone l3-in
set vif vif2 zone l3-in
set vif vif3 zone l3-out
set vif vif4 zone l3-in
set vif vif1 ip 1.2.2.1 netmask 255.255.255.0
set vif vif2 ip 1.2.3.1 netmask 255.255.255.0
set vif vif3 ip 1.1.1.1 netmask 255.255.255.0
set vif vif4 ip 1.2.4.1 netmask 255.255.255.0
set vif vif1 filters enable web,telnet,ping
set vif vif2 filters enable web,telnet,ping
set vif vif3 filters enable web,telnet,ping
set vif vif4 filters enable web,telnet,ping
```

2. 路由

```
set route ip 0.0.0.0 0.0.0.0 1.1.1.250
```

3. QoS

```
eum set qos-all qos-hr priority 0 type single send 1000 recv 2000
eum set qos-all qos-finance priority 0 type single send 2000 recv 3100
eum set qos-all qos-marketing priority 0 type single send 2000 recv 3100 total 4100
```

4. 策略

```
firewall set policy from l3-in to l3-out src-addr 1.2.2.0/24 dst-addr ANY service ANY action permit bandwidth qos-hr status enable

firewall set policy from l3-in to l3-out src-addr 1.2.3.0/24 dst-addr ANY service ANY action permit bandwidth qos-finance status enable

firewall set policy from l3-in to l3-out src-addr 1.2.4.0/24 dst-addr ANY service ANY action permit bandwidth qos-marketing status enable
```

WEB 配置

WEB 的配置与 CLI 的配置相对应：

1. 接口

进入 **网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)->Vif1**，修改 zone 为 l3-in ，提交之后再点击 “**Set VIF IP**”按钮，添加 IP 地址 1.2.2.1/24。

修改虚拟接口　　提交　取消　返回

虚接口名称	vif1	物理口/汇聚接口	lan1	有效	○ 是 ⦿ 否
VLAN	1	区域	l3-in		
加VLAN标签	☐	工作模式	路由模式		
地址转换	☐ 启用				
报文允许	☑ web ☑ telnet ☐ ssh ☑ ping ☐ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 设备认证				
设置虚接口IP	IP 地址:				

图163.　　接口1

同理配置虚拟接口 vif2、vif3 和 vif4，结果如下：

虚拟接口 新增

序号	名称	物理接口/汇聚口	VLAN	IP地址1/掩码	工作模式	区域	有效	操作
共 9 条记录 当前第 1 页								
1	vif0	lan0	1		透明模式	l2-in	是	
2	vif1	lan1	1		路由模式	l3-in	否	
3	vif2	lan2	1		路由模式	office	否	
4	vif3	lan3	1		透明模式	l2-out	是	
5	vif4	lan4	1		透明模式	l2-in	是	
6	vif5	lan5	1		透明模式	l2-in	是	
7	vif6	lan6	1		透明模式	l2-in	是	
8	vif7	lan7	1		透明模式	l2-in	是	
9	vif9	wan0	1		透明模式	l2-in	是	

图164. 接口2

2. 路由

进入 **网络配置(NETWORK)->路由配置(Routing)->网络路由(Static Routing)->新增(Create New)**，添加一条到 1.1.1.250 的默认路由：

新增网络路由表 提交 取消 返回

IP地址	0.0.0.0	子网掩码	0.0.0.0
网关/ISP	1.1.1.250		
*IP地址 0.0.0.0 掩码 0.0.0.0 代表缺省路由			

图165. 路由

3. QoS

进入 **系统配置管理(SYSTEM)->Object->QoS->新增(CreateNew)**，创建一个名为 qos-marketing 的 QoS。

新增服务质量 提交 取消 返回

名称	qos-marketing		
注释			
优先级	0 (7最高,0最低)	类型	带宽限制
发送(Kbits/s)	最大: 2000		
接收(Kbits/s)	最大: 3100		
总共(Kbits/s)	最大: 4100		
群组共享	☐		

图166. QoS

同理分别创建 qos-hr 和 qos-finance 的 参数，结果如下：

服务质量 新增

	名称	优先级	发/收/总带宽(Kbits/s)	类型	操作
共 6 条记录					
	normal-qos	0	max:1000KB/2.0MB/2.4MB	群組共享	
▶	tunnel-qos	0	max:1000KB/2.0MB/2.4MB	通道带宽	
	qos-hr	0	max:1000KB/2.0MB/0KB	带宽限制	
	qos-finance	0	max:2.0MB/3.0MB/0KB	带宽限制	
	qos-marketing	0	max:2.0MB/3.0MB/4.0MB	带宽限制	

图167. QoS

4. 策略

进入**安全(SECURITY)-> 安全策略(Policies)->新增(Create New)**，分别为三个部门配置策略。

（1） 三个部门的员工不能互访

由于三个部门都在安全区 l3-in 里，所以只要将“l3-in—>l3-in”的所有服务都 DENY，就可以了。配置如下：

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 [ ] 之前 ⦿ 最后		
安全区			
源安全区	l3-in	目的安全区	l3-in
地址/用户/地址簿			
⦿ 源 地址 ○ 用户 ○ 地址簿			
⦿ 目的地址 ○ 用户 ○ 地址簿			
动作	DENY	服务	ANY
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☐ 显示高级	

（2） 人力资源部门访问外网

人力资源部门员工的源 IP 为 1.2.2.0/24，访问外网时上行带宽限制为 1M，下行带宽限制为 2M。配置如下：

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 [ ] 之前 ⦿ 最后		
安全区			
源安全区	l3-in	目的安全区	l3-out
地址/用户/地址簿			
⦿ 源 地址 ○ 用户 ○ 地址簿		1.2.2.0/24	
⦿ 目的地址 ○ 用户 ○ 地址簿			
动作	PERMIT	服务	ANY
日志	☐ log		
使能	⦿ 启用 ○ 禁用	☑ 显示高级	
组			
源组		目的组	
定时计划		安全配置	
总服务质量	qos-hr		
监控	☐ 源 ☐ 目的	监控当前连接	☐
流量统计	☐		
注释			

图168. 策略

（3） 财务部门访问外网

财务部门的源 IP 为 1.2.3.0/24，访问外网时上下行双向带宽总和不能超过 2M。配置如下：

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 [ ] 之前 ⦿ 最后		
安全区			
源安全区	l3-in	目的安全区	l3-out
地址/用户/地址簿			
⦿ 源 地址 ○ 用户 ○ 地址簿		1.2.3.0/24	
⦿ 目的地址 ○ 用户 ○ 地址簿			
动作	PERMIT	服务	ANY
日志	☐ log		
使能	⦿ 启用 ○ 禁用	☑ 显示高级	
组			
源组		目的组	
定时计划		安全配置	
总服务质量	qos-finance		
监控	☐ 源 ☐ 目的	监控当前连接	☐
流量统计	☐		
注释			

图169. 策略

（4） 市场部门访问外网

市场部门的员工访问外网时上行带宽最大为 2M，下行带宽最大为 3M，但双向带宽总和不能超过 4M。配置如下：

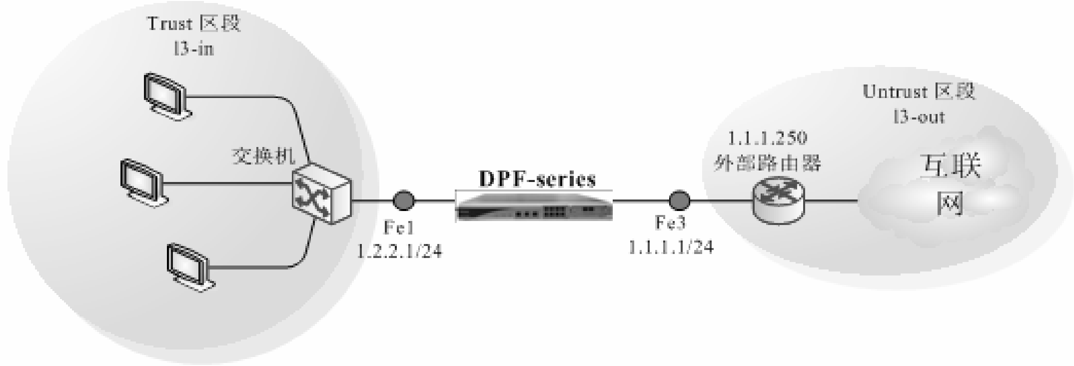
新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 [ ] 之前 ⦿ 最后		
安全区			
源安全区	l3-in	目的安全区	l3-out
地址/用户/地址簿			
⦿ 源 地址 ○ 用户 ○ 地址簿		1.2.4.0/24	
⦿ 目的地址 ○ 用户 ○ 地址簿			
动作	PERMIT	服务	ANY
日志	□ log		
使能	⦿ 启用 ○ 禁用	☑ 显示高级	
组			
源组		目的组	
定时计划		安全配置	
总服务质量	qos-marketing		
监控	□ 源 □ 目的	监控当前连接	□
流量统计	□		
注释			

图170. 策略

16.5 范例：基于策略的通道带宽控制

某公司要求无论网络空闲还是繁忙，都要保证收发邮件和上网的顺畅。公司通向互联网的上行带宽最大为 3M，下行带宽最大为 4M，总带宽不超过 6M。

采用策略中引用通道带宽来实现， 配置通道带宽的上行、下行和总的最大带宽分别为：3M、4M 和 6M；配置 HTTP 服务的保障带宽为：上行 1M，下行 1M，总带宽 2M；配置收发邮件服务的保障带宽为：上行 1M，下行 1.5M，总 2.4M；最小带宽都设置为 0。



CLI

1. 接口

```
set vif vif0 zone l3-in
set vif vif2 zone l3-out
set vif vif0 ip 1.2.2.1 netmask 255.255.255.0
set vif vif0 filters enable web,telnet,ssh,ping,snmp
set vif vif2 ip 1.1.1.1 netmask 255.255.255.0
set vif vif2 filters enable web,telnet,ssh,ping,snmp
```

2. 路由

```
set route ip 0.0.0.0 0.0.0.0 1.1.1.250
```

3. QoS

```
eum set qos-all tunnel-qos priority 0 type total send 3100 recv 4100 total 6100

eum set qos-tunnel tunnel-qos sub tunnel-qos-mail priority 1 max-send 3100 max-recv 4100 max-total 6100 guarantee-send 1000 guarantee-recv 1000 guarantee-total 2000
```

eum set qos-tunnel tunnel-qos sub tunnel-qos-web priority 1 max-send 3100 max-recv 4100 max-total 6100 guarantee-send 1000 guarantee-recv 1500 guarantee-total 2500

eum set qos-tunnel tunnel-qos sub tunnel-qos_others priority 0 max-send 3100 max-recv 4100 max-total 6100

4. 策略

firewall set policy from l3-in to l3-out src-addr ANY dst-addr ANY service HTTP action permit bandwidth tunnel-qos-web status enable

firewall set policy from l3-in to l3-out src-addr ANY dst-addr ANY service POP3 action permit bandwidth tunnel-qos-mail status enable

firewall set policy from l3-in to l3-out src-addr ANY dst-addr ANY service SMTP action permit bandwidth tunnel-qos-mail status enable

firewall set policy from ANY to ANY src-addr ANY dst-addr ANY service ANY action permit bandwidth tunnel-qos_others status enable

WEB 配置

WEB 的配置与 CLI 的配置相对应：

1. 接口

进入 **网络配置(NETWORK)->网络接口(Interfaces)->虚拟接口(Virtual)->vif0**，修改 zone 为 l3-in，提交之后再点击 “**Set VIF IP**”按钮，添加 IP 地址 1.2.2.1/24。

修改虚拟接口　　提交　取消　返回

虚接口名称	vif0	物理口/汇聚接口	fe0		
VLAN	1	区域	l3-in		
有效	⦿ 是 ○ 否	路由环回检查	○ 是 ⦿ 否	源mac地址检查	○ 是 ⦿ 否
加VLAN标签	☐	工作模式	路由模式	安全级别	1
地址转换	☐ 启用				
报文允许	☑ web ☑ telnet ☑ ssh ☑ ping ☑ snmp ☐ 全选				
认证开关	☐ web认证 ☐ 802.1认证 ☐ 设备认证				
VLAN标签过滤	☑ 允许带VLAN标签报文 ☑ 允许不带VLAN标签报文 ☑ 允许带优先级标签报文				
设置虚接口IP	IP 地址:1.2.2.1/24,				

图171.　　接口1

同理配置虚拟接口vif3，结果如下：

虚拟接口　　新增

序号	名称	物理接口/汇聚口	VLAN	IP地址1/掩码	工作模式	区域	有效	操作
共 12 条记录 当前第 1 页								
1	vif0	fe0	1	1.2.2.1/24	路由模式	l3-in	是	
2	vif1	fe1	1		透明模式	l2-in	是	
3	vif2	fe2	1	1.1.1.1/24	路由模式	l3-out	是	
4	vif3	fe3	1		透明模式	l2-in	是	
5	vif4	fe4	1		透明模式	l2-in	是	
6	vif5	fe5	1		透明模式	l2-in	是	
7	vif6	fe6	1		透明模式	l2-in	是	
8	vif7	fe7	1		透明模式	l2-in	是	
9	vif10	ge2	1		透明模式	l2-in	是	
10	vif8	ge0	1		透明模式	l2-in	是	
11	vif9	ge1	1		透明模式	l2-in	是	
12	vif11	ge3	1		透明模式	l2-in	是	

图172.　　接口2

2. 路由

进入 **网络配置(NETWORK)->路由配置(Routing)->网络路由(Static Routing)->新增(Create New)**，添加一条到 1.1.1.250 的默认路由：

新增网络路由表			提交 取消 返回
IP地址	0.0.0.0	子网掩码	0.0.0.0
网关/ISP	1.1.1.250		
*IP地址 0.0.0.0 掩码 0.0.0.0 代表缺省路由			

图173. 路由

3. QoS

进入 **系统配置管理(SYSTEM)->Object->QoS->新增(CreateNew)**，创建一个名为"tunnel-qos"的通道带宽

Edit QoS			提交 取消 返回
名称	tunnel-qos		
注释			
优先级	0 (7最高,0最低)	类型	通道带宽
发送(Kbits/s)	最大: 3100		
接收(Kbits/s)	最大: 4100		
总共(Kbits/s)	最大: 6100		

图174. 通道带宽

分别创建 两个子带宽 qos-mail 和 qos-web 的 参数，结果如下：

服务质量					新增
	名称	优先级	发/收/总带宽(Kbits/s)	类型	操作
共 4 条记录					
▼	tunnel-qos	0	max:3.0MB/4.0MB/6.0MB	通道带宽	
	tunnel-qos-mail	1	guarantee:1000KB/1000KB/2.0MB	子带宽	
	tunnel-qos-web	1	guarantee:1000KB/1.5MB/2.4MB	子带宽	
	tunnel-qos_others	0	guarantee:0KB/0KB/0KB	子带宽	

图175. QoS

4. 策略

进入**安全(SECURITY)-> 安全策略(Policies)->新增(Create New)**，配置策略保证web和邮件服务。

配置策略为HTTP服务提供保障带宽：上行1000K，下行1000K，总2M。

策略修改 匹配计数:0			提交 取消 返回
源安全区	l3-in	目的安全区	l3-out
地址/用户/地址簿			
	⦿ 源地址 ○ 用户 ○ 地址簿	ANY	
	⦿ 目的地址 ○ 用户 ○ 地址簿	ANY	
动作	PERMIT	服务	HTTP
日志	☐ log		
使能	⦿ 启用 ○ 禁用	☑ 显示高级	
组			
源组	ANY	目的组	ANY
定时计划		安全配置	
总服务质量	tunnel-qos-web		
监控	☐ 源 ☐ 目的	监控当前连接	☐
流量统计	☐		
注释			

图176. 策略引用tunnel-qos-web

同理邮件服务配置策略提供保障带宽：上行1000K，下行1.5M，总2.4M。

最后配置一条策略给所有的服务，引用tunnel-qos-others。

策略修改 匹配计数:0 提交 取消 返回

源安全区	ANY	目的安全区	ANY
地址/用户/地址簿			
	⊙ 源地址 ○ 用户 ○ 地址簿	ANY	
	⊙ 目的地址 ○ 用户 ○ 地址簿	ANY	
动作	PERMIT	服务	ANY
日志	☐ log		
使能	⊙ 启用 ○ 禁用	☑ 显示高级	
组			
源组	ANY	目的组	ANY
定时计划		安全配置	
总服务质量	tunnel-qos_others		
监控	☐ 源 ☐ 目的	监控当前连接	☐
流量统计	☐		
注释			

图177. 策略引用tunnel-qos-others

注意：使用通道策略必须在最后配置一条引用others子带宽的策略，才能保证其他服务的使用

配置策略列表如下：

策略列表: All

新增 ☐ 全选 提交 清空

序号	源地址/用户/地址簿	目的地址/用户/地址簿	定时计划	安全配置	服务	匹配计数	动作	状态	操作
▼ l3-in -> l3-out 共 3 条记录									清除
1	ANY	ANY			HTTP	0	permit	☑	
2	ANY	ANY			POP3	0	permit	☑	
3	ANY	ANY			SMTP	0	permit	☑	
▼ 全局 共 1 条记录									清除
1	ANY	ANY			ANY	0	permit	☑	

图178. 策略

。

17 主机管理

17.1 简介

为了方便管理和查询，DPF-Series 设备支持对用户(包括认证用户和静态用户)的 IP 流量进行统计，对在线用户进行查询和在线用户流量排名。详细功能如下：

- 用户流量统计： 以用户名为索引的所有用户(认证和静态)的流量统计
- IP 流量统计： 以 IP 地址为索引的所有用户(认证和静态)的流量统计
- 在线静态用户： 可以查询到所有在线静态用户的详细信息
- 在线认证用户： 可以查询到所有在线认证用户的详细信息
- 在线用户流量排名： 可以查询到所有在线用户(认证和静态)中，流量排前 10/20/30/40/50 名用户的详细信息，并按照流量从大到小的顺序排列
- 用户上网记录： 可以查询所有用户(认证和静态)上网的统计信息，包括用户名、主机名、登录时间、退出时间、IP 地址和 MAC 地址

17.2 范例：流量统计

DPF-Series 设备支持将用户的流量信息发送到 Syslog 服务器上，IP Address 就是 Syslog 服务器地址，Port 为服务器接收 Syslog 的端口号，一般用 514。

进入 USER->Users->**Statistics**，配置.

用户信息统计，不光是对认证和静态用户统计，还可以对不需要认证的用户进行统计，这就需要配置想要统计的用户的 IP 地址范围。同时可以限制用户的带宽和 Session 数，也可以为这些用户绑定黑名单功能。这样也可以控制不需要认证的用户对网络的访问情况。如下，统计人力资源部的员工访问网络的流量，同时限制带宽和启用黑名单功能。

进入 **USER->Users->Statistics->Subnet Statistics->新增(CreateNew)**，输入以下内容：

新增子网配置			提交 取消 返回
名称			
起始IP	1.2.2.5	掩码	1.2.2.50
IP统计	○ 启用 ⦿ 禁用		
上行服务质量	2M	下行服务质量	3M
源会话数	0	目的会话数	0
黑名单控制			
P2P服务质量			
P2P上行服务质量		P2P下行服务质量	
P2P新建会话速率	0	P2P会话限制	0
计划			

图179. 新建流量统计

DPF-Series 设备支持根据用户的用户名或 IP 地址来统计流量。

进入 **USER->Users->Statistics->Subnet Statistics->User Statistics**，即可显示根据用户名来统计的查询结果.

进入 Usr**R->Users->Statistics->Subnet Statistics->IP Statistics**，即可显示根据 IP 来统计的查询结果.

点击某个用户的“**detail**”按钮(鼠标指示的位置)，可以查看到此用户的详细信息

详细信息包括一整年(1 月～12 月)、每个季度、每个月和每天的流量统计信息。

点击某个用户的“**clear**”按钮(鼠标指示的位置)，可以清除此用户的统计信息，所有的流量信息重新开始统计。

点击某个用户的“**delete**”按钮(鼠标指示的位置)，可以删除此用户的统计信息，

17.3 范例：查看在线静态用户

DPF-Series 设备支持通过过滤条件来查询在线的静态用户，可以根据用户组，用户名和用户的 IP 来查询。查询的结果可以根据用户的 IP 地址或用户名来排序。如果是按 IP 来排序，则是按照 IP 从小到大的顺序排列；如果是按照用户名来排序，则根据用户名的首字母来排序。

17.4 范例：查看在线认证用户

进入 **USER->Users->Online A-users**，可以查询到所有在线认证用户的详细信息。方法和在线静态用户一样，这里不再叙述。

17.5 范例：在线用户流量排名

进入 **USER->Users->Traffic Ranking**，可以对所有在线用户进行流量排名。可以根据需要，选择所要查看的名次数目，可以选择前 10/20/30/40/50 名，查询的结果按流量从大到小排列。

17.6 范例：查看用户上网统计

DPF-Series 设备可以查询到用户登录和退出的时间，以及 IP 地址、MAC 地址和主机名。值得注意的是用户至少要下线一次，才能查到此信息。可以输入想要查询的用户名、主机名、时间范围、MAC 地址等参数来过滤查询信息。不输入任何参数就是查询所有的用户。缺省情况下，查询到的所有信息按照 IP 地址降序排列，也可以选择按照升序来排列。

18 IM & P2P

18.1 简介

IM

在 IM 日益成为一个难以替代的交流工具的同时，这项技术也承受着安全方面的考验。非授权的 IM 使用不但会降低企业的生产率，也可能会造成机密文件的泄漏。更为严重的是 IM 漏洞、木马和病毒层出不穷，给用户的资料安全带来严重威胁。

DPF-Series 竭力平衡 IM 的优缺点，提供了细致的 IM 控制功能。

- 完全拒绝某个(些)IM 软件的使用
- IM 部分功能的限制（仅对 MSN, ICQ/AIM/Yahoo!有效）
- 分时段控制：比如 9：00～12：00 和 14：00～18：00 是上班时间，不允许某些员工使用 IM 软件，其它时间可以使用。
- 对单个 IP(或者用户) 进行单独控制
- IM 完善的日志记录、聊天记录

当启用 IM 的日志功能后，可以记录用户使用 IM 软件的一些信息，包括：

- 登录某种 IM 软件用户名和时间
- 传输文件的时间和文件名
- 查看聊天记录
- 传输语音/视频的时间

P2P

以 BT、Edonkey 和 PPLIVE 为代表的 P2P(点对点)互联网文件传输协议和网络电视，由于其传输速度快，匿名与及文件查找方便等特点，成为了互联网用户传输和共享大容量文件（尤其是影音文件）的首选。然而，缺乏有效的管理和控制，不但占用巨大网络带宽和连接会话数，而且严重影响其他用户的正常网络使用。据统计，P2P 的流量在许多网内已经占到总流量的 60％－80％，给企业正常业务的开展造成影响。另外，P2P 的使用，给企业带来了严重的安全问题和损失。为了帮客户应对 P2P 带来的日益严重的问题，DPF-Series 设备提供完备的 P2P 的管理功能。

DPF-Series 设备对 P2P 的管理控制包括以下几个方面：

- 完全拒绝某个(些) P2P 软件的使用
- 带宽控制：允许某个(些) P2P 软件的使用，但对用户流量带宽进行限制
- 会话数控制：允许某个(些) P2P 软件的使用，但对用户会话数进行限制
- 分时段控制：比如 9：00～12：00 和 14：00～18：00 是上班时间，不允许员工使用 P2P 软件，其它时间可以使用 P2P 软件，但是每个人使用 P2P 的带宽只能是 100 K。
- 对单个 IP(或者用户) 进行单独控制
- P2P 完善的流量统计

18.2 范例

本例列举的是一个软件公司，允许开发部门使用 QQ/TM，只允许用 MSN 来聊天，禁止使用其它 IM 工具，并启用 IM 日志功能。同时禁止开发部门使用 BT 和 Emule 两种 P2P 软件，WEB 配置如下：

1. 配置 P2P 控制列表

进入 **IM/P2P/L7->Setting ->P2P/ P2P-TV**，可以看到系统默认创建的两条配置。denyall 是禁止使用所有的 P2P 软件，permitall 是允许使用所有的 P2P 软件。

为开发部门增加一个 P2P 控制列表，禁止开发部门使用 BT 和 Emule。如下：

新增IM　提交　取消　返回

IM 名称：imdevelop

协议类型	版本	拒绝服务类型	日志
MSN	8.0	☐ 全部 ☐ 文字聊天 ☑ 语音聊天 ☑ 文件传输	☑
QQ/TM	2006B2	☐ 全部	☑
AIM/ICQ	icq5,aim5.9	☑ 全部 ☑ 文字聊天 ☑ 语音聊天 ☑ 文件传输	☑
YMSG	7.0	☑ 全部 ☑ 文字聊天 ☑ 语音聊天 ☑ 文件传输	☑
Jabber/google-talk	Gaim1.50	☑ 全部	☑
POPO	2004	☑ 全部	☑
UC	2005III	☑ 全部	☑
ET	4.0	☑ 全部	☑
WANGWANG	1.5B1	☑ 全部	☑

图180.　p2p 配置

2. 配置 IM 控制列表

进入 **IM/P2P/L7->Setting ->IM**，可以看到系统默认创建的两条配置，denyall 是禁止使用所有的 IM 软件，permitall 是允许使用所有的 IM 软件。

为开发部门增加一个 IM 控制列表，允许开发部门使用 QQ/TM、MSN 只允许聊天，禁止使用其它 IM 工具，同时启用日志功能。

3. 安全配置

进入 **安全(SECURITY)->SECURITY Setting**，创建开发部门的安全配置参数。启用 IM Profile (选择 imdevelop) 和 P2P Profile (选择 p2pdevelop)。

4. 引用安全配置

进入 **安全(SECURITY)->安全策略(Policies)->新增(Create New)**，在策略中引用安全配置，如下：

新增安全策略　提交　取消　返回

位置	○ 置顶 ○ 在 ＿＿ 之前 ◉ 最后		
安全区			
源安全区	l2-in	目的安全区	l2-out
地址/用户/地址簿			
	◉ 源 地址 ○ 用户 ○ 地址簿	1.2.2.100-1.2.2.200	
	◉ 目的地址 ○ 用户 ○ 地址簿		
动作	PERMIT	服务	ANY
日志	☐ log		
防病毒	☐ 防病毒		
使能	◉ 启用 ○ 禁用	☑ 显示高级	
组			
源组		目的组	
定时计划		安全配置	
双向服务质量			
上行服务质量		下行服务质量	
流量统计	☐		
注释			

图181.　引用安全配置

18.3 P2P 流量控制

服务质量(QoS)或者说带宽控制是指为用户或应用程序分配适当的网络带宽数量。DPF-Series 设备可以单独对 P2P 流量进行带宽控制，用来调整流经 DPF-Series 设备的 P2P 信息流的速率。

DPF-Series 配置拥有两种带宽控制方法：

- 基于用户
  用来控制每个用户的 P2P 流的带宽。在 P2P 配置中指定 User Qos Enable，那么本配置就会使用用户级的 P2P 带宽控制，即每个用户都拥有独立的 P2P 带宽。
- 基于策略
  在 P2P 配置中指定有效的 Qos Profile，但不指定 User Qos Enable，然后在安全配置中引用这个 P2P 配置，最后在策略中引用该安全配置。那么本配置就会使用策略级带宽控制，也就是所有受此策略控制的 P2P 流最大带宽为 Qos Profile 指定的带宽。

如果基于用户和基于策略的带宽配置重叠时，以其中带宽小的为准。

更详细地，基于用户级的带宽是针对每个用户来进行带宽限制的。例如：某个授权策略里引用上行和下行都是 1M 的 QoS，那么所有引用这个授权策略的用户最大都有 1M 的带宽。而基于策略级的 QoS 是指所有符合这条策略的流最大带宽为 QoS 指定的带宽。例如，配置源 IP 是 1.1.1.1～1.1.1.10 的 QoS 为 2M 的策略，那么源 IP 为 1.1.1.1～1.1.1.10 的所有流最大有 2M 的带宽。

范例

本例列举的是一个软件公司，开发部门只允许使用 BT 和 emule 两种 P2P 软件，并限制带宽。开发部的 IP 地址为：1.2.2.100-1.2.2.200。为简单起见，这里省去与用户认证相关的其它配置，只列举与 P2P QoS 相关的配置。关于认证用户与授权策略之间的调用关系请参见“**用户认证**”章节的 QoS。

1. QoS
   DPF-Series 设备设置了三个默认的 QoS 参数 (UNLIMIT、1M 和 10M)。
   进入 **系统配置管理(SYSTEM)->Object->QoS->新增(Create New)**，创建一个名为 6K 的 QoS。创建完成后，结果如下：

服务质量设置　　新增

序号	名称	优先级	带宽(Kbit/s)	群组共享	操作
共 7 条记录					
1	1M	2	1000	No	
2	10M	1	10000	No	
3	UNLIMIT	0	10000000	No	
4	2M	0	2000	No	
5	3M	0	24000	No	
6	4M	0	32000	No	
7	6K	0	6	No	

图182.　　QoS

2. 授权策略
   进入 **USER->Group Info->Authorization**，修改默认的授权策略 normal。P2P QoS 选择 6K，Outbound QoS 和 Inbound QoS 选择 1M。
   【下面的配置达到的效果为：调用此授权策略的用户的 P2P 信息流单独最大有 6K 的带宽，其它信息流最大有 1M 的带宽】

新增授权策略			提交 取消 返回
名称	normal		
注释	default normal athr policy		
上行服务质量	1M	下行服务质量	1M
源会话	50	目的会话	50
P2P服务质量	2M		
P2P上行服务质量		P2P下行服务质量	
P2P新建会话速率	0	P2P会话限制	0
定时计划		超出计划设置	☐

图183.　　修改授权策略

【如果 P2P QoS 选择 "UNLIMIT"，Outbound QoS 和 Inbound QoS 选择 1M；那么调用此授权策略的用户的所有信息流（包括 P2P）最大有 1M 的带宽】.

【如果 P2P QoS 选择 6K，Outbound QoS 和 Inbound QoS 选择"UNLIMIT"；那么调用此授权策略的用户的 P2P 信息流单独最大有 6K 的带宽，其它信息流不受限制】，如下：

修改授权策略			提交 取消 返回
名称	normal		
注释	default normal athr policy		
上行服务质量	UNLIMIT	下行服务质量	UNLIMIT
源会话	50	目的会话	50
P2P服务质量	6K		
P2P上行服务质量		P2P下行服务质量	
P2P新建会话速率	0	P2P会话限制	0
定时计划		超出计划设置	☐

图184.　　修改授权策略

3. P2P 控制列表

可以只启用策略级或者用户级的 QoS，也可以二者都启用或者都不启用，如果二者都启用，则最小的 QoS 起作用。

进入 **IM/P2P/L7->Setting ->P2P/P2P-TV/L7**，修改 P2P 控制列表 p2pdevelop，启用策略级和用户级的 QoS。

【为了使截图简洁，此图去掉了其它不相关的 P2P 软件，重点显示 emule 和 BT。】

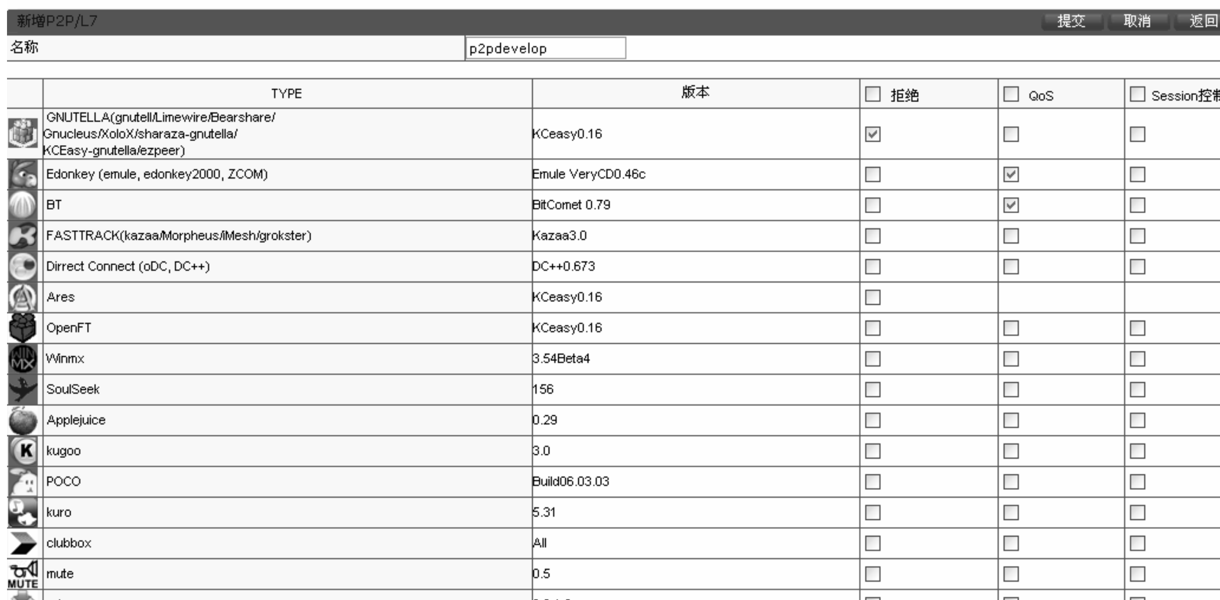


图185.　　启用 P2P QoS

4. 安全配置

   进入 **安全(SECURITY)->SECURITY Config**，引用 P2P 控制列表，如下：

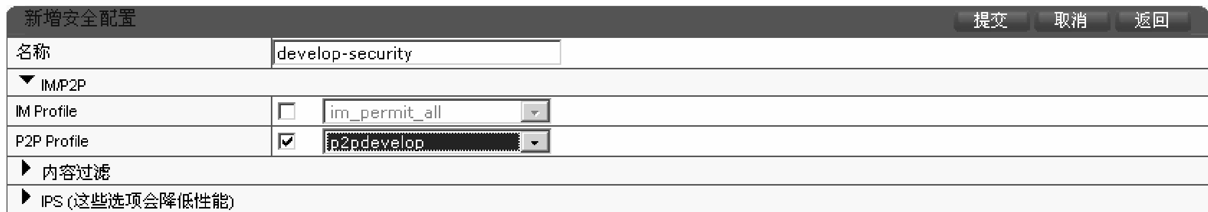


图186.　　安全配置

5. 引用安全配置

   进入 **安全(SECURITY)->安全策略(Policies)->新增(Create New)**，在策略中引用安全配置。

18.4 统计

为了方便管理和查询，DPF-Series 设备支持对用户的 IM/P2P 流量进行统计。详细功能如下：

- 在静态用户： 统计静态用户的详细信息
- 认证用户： 统计认证用户的详细信息
- 非认证（静态）用户：统计不需要认证的用户的详细信息。这就需要配置想要统计的用户的 IP 地址范围。

范例

IM 的统计功能自动启用。要统计 P2P 的信息，首先要启用 P2P 的 QoS。如果是对认证用户和静态用户进行统计，就启用 User Qos，对不需要认证的用户信息进行统计，就启用 Qos Profile。如果要对所有用户进行统计，就将二者都启用。具体的配置如下：

1. 启用 P2P 的统计功能

   进入 **IM/P2P/L7->Setting ->P2P/P2P-TV/L7**，修改某个 P2P 条目的配置，这里启用 User Qos 和

Qos Profile。

2. 配置统计用户

P2P 用户信息统计，不光是对认证和静态用户统计，还可以对不需要认证的用户进行统计，这就需要配置想要统计的用户的 IP 地址范围。这和**“用户认证”**一节的统计是一样的，可参照**“用户认证”**一节。

进入 **USER->Users->Statistics->Subnet Statistics->新增(CreateNew)**，输入以下内容：

新增子网配置			提交 取消 返回
名称	develop		
起始IP	172.16.161.60	掩码	172.16.161.250
IP统计	○ 启用 ⦿ 禁用		
上行服务质量	1M	下行服务质量	1M
源会话数	0	目的会话数	0
黑名单控制			
P2P服务质量			
P2P上行服务质量		P2P下行服务质量	
P2P新建会话速率	0	P2P会话限制	0
计划			

图187. 新建流量统计

3. IM/P2P 统计查询

进入 **IM/P2P/L7->Statistics->Summary，**可以看到 IM/P2P 的统计信息。图的上部分显示了总的 session、总的 packet 等信息。下面的 Summary 是每隔 5 分钟统计一次，列举了 5 分中内 IM/P2P 的新的 session 数、P2P 的报文数、按字节计算的 P2P 的流量。

总计			
总会话	0	总丢弃会话	0
总流量	0KB	总封包	0

Summary（清除 历史）

时间序列(5分钟)	时间	IM/P2P总新会话数	IM/P2P总丢弃会话数	P2P封包数	P2P流量	操作
Page:1						
1	2007-04-30 16:45	0	0	0	0KB	
2	2007-04-30 16:40	0	0	0	0KB	
3	2007-04-30 16:35	0	0	0	0KB	
4	2007-04-30 16:30	0	0	0	0KB	
5	2007-04-30 16:25	0	0	0	0KB	
6	2007-04-30 16:20	0	0	0	0KB	
7	2007-04-30 16:15	0	0	0	0KB	
8	2007-04-30 16:10	0	0	0	0KB	
9	2007-04-30 16:05	0	0	0	0KB	
10	2007-04-30 16:00	0	0	0	0KB	

图188. 查看 IM/P2P 统计信息

点击上图右边操作栏的**“详细”**按钮（粉色框所示），可以查看到更加详细的统计信息：

Category Summary

序号	IP	新会话	丢弃会话	登陆次数	文字信息	语音	文件传
共 42 条记录							
1	msn	0	0	0	0	0	0
2	aim	0	0	0	0	0	0
3	ymsg	0	0	0	0	0	0
4	qq	0	0	0	N/A	N/A	N/A
5	jabber	0	0	0	N/A	N/A	N/A
6	popo	0	0	0	N/A	N/A	N/A
7	et	0	0	0	N/A	N/A	N/A
8	uc	0	0	0	N/A	N/A	N/A
9	wangwang	0	0	0	N/A	N/A	N/A
10	gnutella	0	0	0	N/A	N/A	N/A
11	edonkey	0	0	0	N/A	N/A	N/A

图189. 查看 IM/P2P 统计信息

4. 按照 IP 来查询 P2P 统计信息

进入 **IM/P2P/L7->Statistics->IP Statistics**，这是按照 IP 来统计 P2P 的信息：

IP 统计 Clear

序号	IP	用户名	IM/P2P总新会话数	IM/P2P总丢弃会话数	P2P封包数	P2P流量	操作
Total:0 Page:1							

图190. 按照 IP 来统计 P2P 的信息

点击上图右边操作栏的“**详细**”按钮（粉色框所示），可以查看到 IP 为 172.16.161.66 用户每天的统计信息：

IP 统计 Clear

序号	IP	用户名	IM/P2P总新会话数	IM/P2P总丢弃会话数	P2P封包数	P2P流量	操作
Total:0 Page:2							

图191. 查看 IP 为 172.16.161.66 的统计信息

点击上图右边操作栏的“**More**”按钮（粉色框所示），可以查看到某天更加详细的统计信息：

IP Statistics Detail IP:172.16.161.66

Time Sequence in day	Time	IM/P2P total new sessions	P2P Packets	Traffic(KByte)	More...
Total:2 Page:1					
1	2006-6-25	7	676	515	▶
2	2006-6-23	78	11826	8610	▼

Index	IP	Session count	Login Count	Chats messages	Voice messages	Transfer files
IP:172.16.161.66 User name: Total:2						
1	msn	24	7	1843	0	0
2	aim	0	0	0	0	0
3	ymsg	228	8	1254	0	0
4	qq	0	0	N/A	N/A	N/A
5	jabber	0	0	N/A	N/A	N/A
6	popo	0	0	N/A	N/A	N/A
7	et	0	0	N/A	N/A	N/A
8	uc	0	0	N/A	N/A	N/A
9	wangwang	0	0	N/A	N/A	N/A
10	gnutella	0	0	N/A	N/A	N/A
11	edonkey	19	0	N/A	N/A	N/A

图192. 查看 IP 为 172.16.161.66 的详细统计信息

19 服务控制

19.1 简介

在流量的统计和管理时，为了区分不同的应用，DPF-Series 设备的服务控制功能提供了多种方法来对上至 7 层的网络协议进行分类、分析和管理。

- 支持对 TCP、UDP、HTTP、ICMP 等协议进行分类统计
- 支持对邮件传输软件、文件传输软件、游戏软件、IM/P2P 软件等一百多种协议进行统计和管理
- 支持流量统计图
- 支持每 5 分钟流量值的统计

19.2 WEB 配置方法

1. 设置需要统计的应用

   进入 **SERVICE CTRL->Setting**，添加要统计和管理的软件。

   这里“**Protocol/IP/Port based**”指基于上至 4 层的统计，而“**Content Based**”指上至 7 层的统计。在添加一个新条目时，只能选择其中之一。

   比如，要统计和管理 POP3、SMTP、FTP 和 TFTP 的信息，那么就点中“**Protocol/IP/Port based**”，选择 POP3、SMTP、FTP 和 TFTP，然后点击“**--->**”按钮，将这四个软件添加到右侧表项，最后点击“**Create Multi**”或者“**Create One**”按钮，就可以创建需要管理和统计的条目。

   如果希望将多个协议进行统一管理和统计，就点击“**Create One**”，这样就会将多个协议创建到一个条目，这时需要在“**name**”处输入一个名字，比如 hr。

   如果希望每个协议单独进行统计和管理，就点击“**Create Multi**”，可以为每个协议创建一个条目，这样可以简化配置。这时就不需要输入“**name**”，系统自动会根据协议的名称生成。

   下面就是添加 POP3、SMTP、FTP 和 TFTP 协议的例子：

新增服务控制			新增多个 新增一个 取消 返回
名称	hr		
带宽	0 (Kbits)	优先级	0 (7最高,0最低)

服务			
	Content Based	msn aim ymsg qq jabber popo et uc wangwang gnutella edonkey bt fasttrack dc skype poco	---> <--- 清除
	Protocol/Ip/Port based	---Predefine Service--- ===Mail-System=== BIFF ccMAIL IMAP2 IMAP3 LotusNotes POP2 SMTP UUCP ===File-Transfer-Syst FTP_CMD MS_RPC NFS Printer Print_Srv	---> <--- 清除

图193.　　添加 Service Control

下面就是点击“**CreateMulti**”之后的结果：

服务控制设置　　启用/禁用全部　提交　新增

序号	Profile	带宽(Kbits)	优先级	服务成员数	状态	删除	操作
共 2 条记录							
1	ftp_data	0	0	1	☑	☐	
2	tftp_data	0	0	1	☑	☐	

图194.　　添加 Service Control

或者点击“**CreateOne**”，结果如下：

服务控制设置　　启用/禁用全部　提交　新增

序号	Profile	带宽(Kbits)	优先级	服务成员数	状态	删除	操作
共 1 条记录							
1	hr	0	0	0	☑	☐	

图195.　　添加 Service Control

1. 查看统计结果

   进入 **SERVICE CTRL->Statistics**，可以查看统计的结果及流量图。



图196.　　　查看流量统计

点击每个协议后面的图标，可以查看此协议近 1 个小时(每 10 秒钟统计一次)和近 36 个小时（每 5 分钟统计一次）的流量统计图。例如，查看 **SMTP** 的统计图：

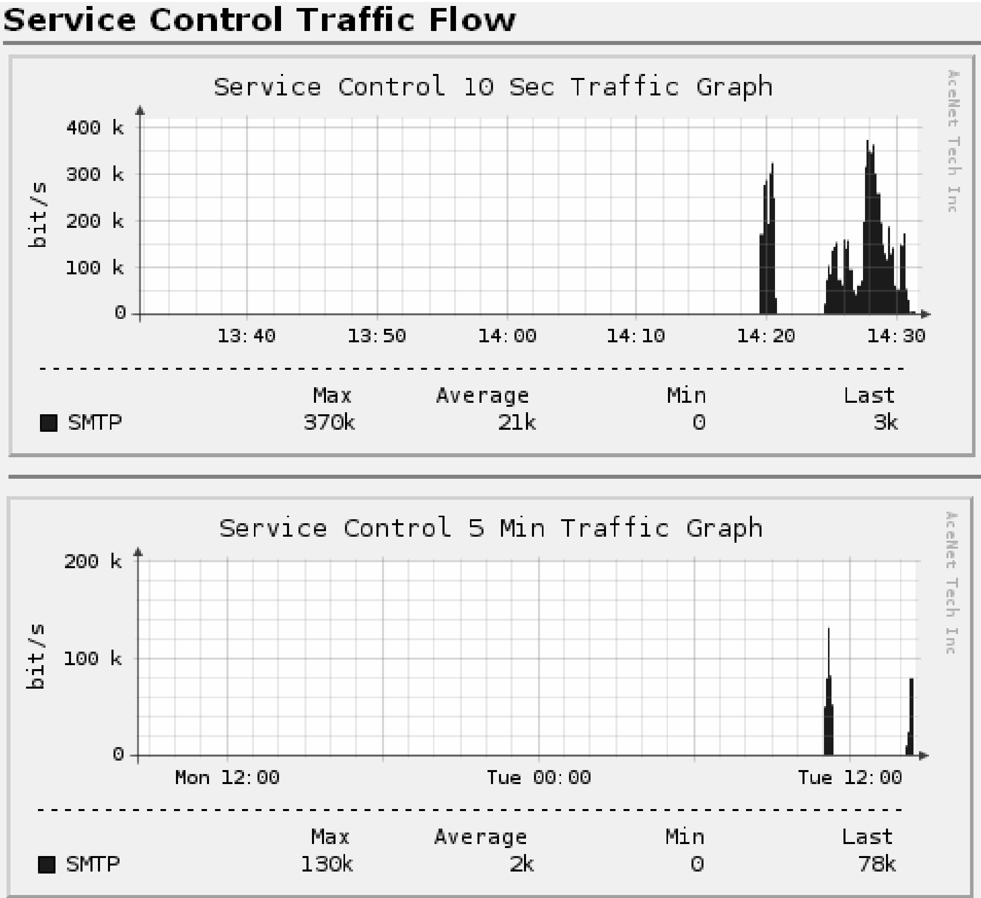


图197.　　　查看流量统计

点击每个协议后面的图标，可以查看每 5 分钟的历史统计信息。

DPF-Series 设备还可以对照几个应用软件之间的流量统计图。比如，要对比 POP3 和 SMTP 的统计图，那么选中 POP3 和 SMTP ，再点击“**--->**”按钮，将 POP3 和 SMTP 添加到右侧表项，然后可以点击“**Graph**”按钮，便可看到 POP3 和 SMTP 的流量对照图；或者点击“**Add**”按钮，将 POP3 和 SMTP 添加到“**Monitor Unit**”中，再点击后面的图标，查询统计信息，这可以方便以后直接查询。

点击“**POP3，SMTP**”后面的图标，查看二者的流量统计对照图：

下面就是查到的“**POP3，SMTP**”的流量统计对照图：

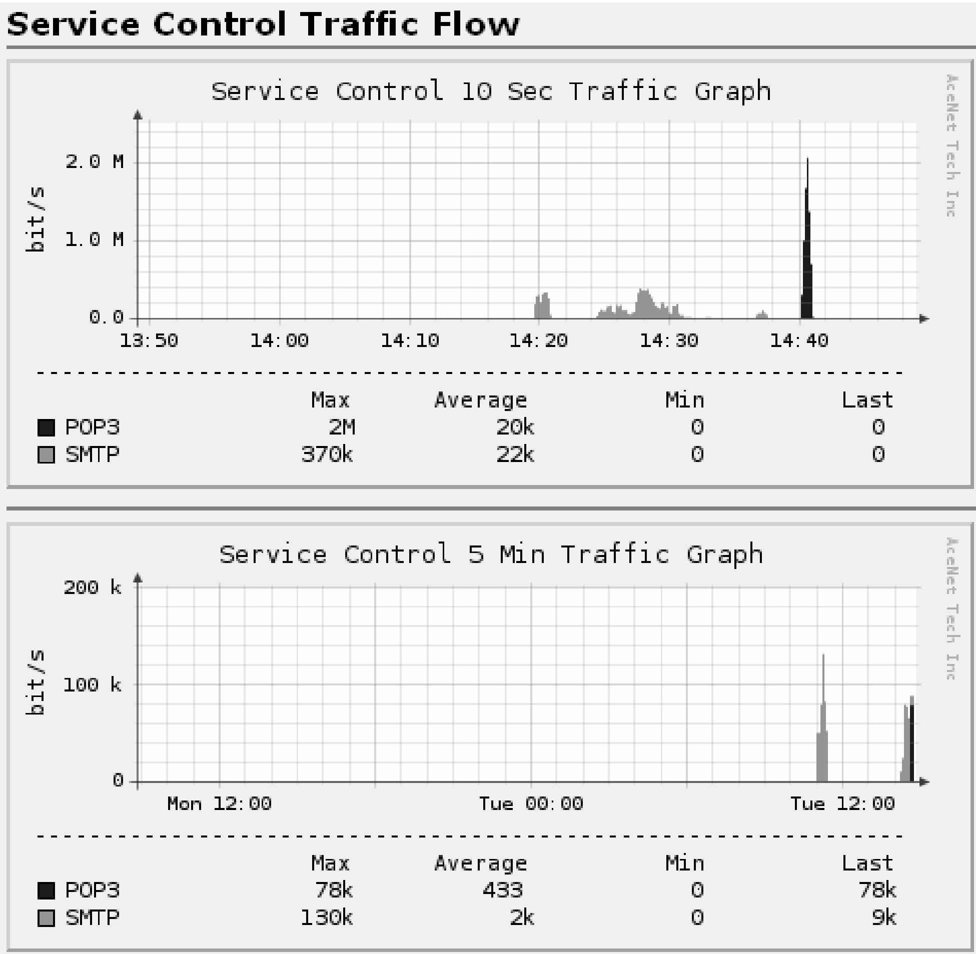


图198. 查看流量统计

20 入侵检测

20.1 简介

入侵防御系统(IPS) 针对企业深层应用进行防御，采用在线检测的模式可以极大地保证采取防御手段的时间，可以对于攻击行为进行防御。

DPF-Series 设备的 IPS 包括：

- ♦ 异常行为检测
- ♦ 扫描攻击

20.2 异常行为检测

进入 **IPS->Anomaly**，可以分别对各个 zone 进行异常行为的防御，下图显示了 DPF-Series 设备可以防御的内容（默认是显示 l3-in 区域的配置）：

安全区域:列表 l3-in

FIREWALL 选项 提交 取消 返回

分片报文	允许 禁止	防止非法IP	启用 禁用
ICMP分片报文	允许 禁止	源路由检查	启用 禁用
TCP SYN分片报文	允许 禁止	UDP校验和检查	启用 禁用
TCP FIN分片报文	允许 禁止	IP选项检查	启用 禁用
TCP RST分片报文	允许 禁止	TCP标志检查	启用 禁用
2层不可知报文	允许 禁止	3层安全检查	启用 禁用
3层不可知报文	允许 禁止	4层安全检查	启用 禁用
IP Option报文	允许 禁止	防止land_attack攻击	启用 禁用
过短分片报文	允许 禁止	防止winnuke攻击	启用 禁用
过长ICMP报文	允许 禁止	防止ping_of_death攻击	启用 禁用
安全区域内转发	允许 禁止	防止tear_drop攻击	启用 禁用
		安全区域绑定检查模式	MAC Vlan 物理端口
IP option过滤设置	禁止IP 宽松源路由选项	禁止IP记录路由选项	禁止IP安全选项
	禁止IP stream选项	禁止IP严格源路由选项	禁止IP时间戳选项
防止分片洪泛攻击		启用 禁用	
防止ICMP洪泛攻击		启用 禁用	
防止UDP洪泛攻击		启用 禁用	
防止TCP SYN洪泛攻击		启用 禁用	
源MAC锁定		启用 禁用	门限值: 3

图199. 异常行为检查

下面对各项进行解释：

- ♦ Fragment
  允许或者禁止所有分片报文通过
- ♦ ICMP Fragment
  允许或者禁止 ICMP 分片报文通过
- ♦ TCP SYN Fragment
  允许或者禁止 TCP SYN 分片报文通过
- ♦ TCP FIN Fragment
  允许或者禁止 TCP FIN 分片报文通过
- ♦ TCP RST Fragment
  允许或者禁止 TCP RST 分片报文通过
- ♦ Unknown L2
  以太网类型为没有定义的报文，例如，以太网类型为 0x0899,0x9910,0xa573 等报文。可以允许或者

禁止此类报文通过

- Unknown L3
  指非 TCP、UDP、ICMP、IGMP 等没有指明类型的 IP 报文，可以允许或者禁止此类报文通过
- IP Option
  允许或者禁止带有 IP 选项的报文通过
- Undersize Fragment
  长度小于系统指定长度的非最后一片分片报文称为过短分片报文，可以允许或者禁止此类报文通过。
  进入 **网络配置(NETWORK)->安全区域(Zones)**，可为系统设置可以接收的最长 ICMP 分片报文和最短分片报文。缺省情况下，分别是 1500 和 512。这是全局的设置，即设置一旦生效就应用于所有 zone

- Oversize ICMP
  长度大于系统指定长度的 ICMP 非分片报文，可以允许或者禁止此类报文通过
- Intra-zone Forwarding
  允许或者禁止报文在此同一安全区域里进行转发
- IP Option Filter
  允许或者禁止某种 IP 选项报文通过
- Prevent Illegal IP
  允许或者禁止非法 IP 报文通过，比如源 IP 为：
  - 127.0.0.0 ～ 127.0.0.255
  - 224.0.0.0 ～ 239.255.255.255
  - 240.0.0.0 ～ 254.255.255.255
- Source Path Check
  启用源路由检查后，当报文进行路由时，禁止报文从入口出去
- UDP Checksum Check
  允许或者禁止带有错误的 UDP 校验和报文通过
- IP Option Check
  对带有 IP 选项或者 TCP 选项的 IP 报文进行检查，如果启用了，选项符合标准则允许通过
- TCP Flag Check
  TCP 中 6 个 bit 的标志位(URG/ACK/PSH/RST/SYN/FIN),它们中可以同时多个为 1 或 0,6 bit 的标志位可以有 64 种组合,但其中只有 20 种（2/10/16/17/18/20/24/25/26/28/34/42/48/49/50/52/56/57/58/60）是合法的，其他的都是不合法的，启用“TCP 标志检查”后，对于不合法的 TCP 报文应该丢弃。
- L3 Sanity Check
  在 3 层允许或者禁止非法的 IP 报文通过，比如以下报文：
  - 带有可选项报文的报文，其中可选项的长度为非法值。
  - IP 报文版本不为 4 的 ip 报文直接丢弃。
  - IP 报文头长小于 20Bytes 报文丢弃。
  - 报文总长度小于报文二层封装头＋IP 报文头长度报文。
  - IPV4 TTL 为 0 报文丢弃。
  - IPV4 报文 IP 报文头 CHECKSUM 错误丢弃
  - 目的 IP 地址为 E 类地址报文丢弃
  - 源 IP 地址为三层多播地址（>=224.0.0.0）的 IP 报文丢弃
- L4 Sanity Check
  在 4 层允许或者禁止非法的 IP 报文通过，比如以下报文：
  - TCP 头长度小于 20Bytes 的报文。
  - TCP CHECKSUM 错误报文。
  - ICMP CHECKSUM 错误的报文。
- Prevent Land Attack

Land 报文是指源 IP 和目的 IP 相同的报文，可以允许或者禁止此类报文通过

- Prevent Winnuke Attack

  WinNuke 是针对互联网上运行 Windows 的任何计算机的 DoS 攻击。攻击者将 TCP 片段（通常发送给设置了紧急(URG) 标志的 NetBIOS 端口 139）发送给具有已建连接的主机。这样就产生 NetBIOS 碎片重叠，从而导致运行Windows 的机器崩溃。

- Prevent Ping of death

  允许的最大 IP 封包长度是 65,535 字节，其中包括长度通常为 20 字节的封包包头。ICMP 回应请求是一个含长度为 8 字节长的伪包头的 IP 封包11。因此，ICMP 回应请求的数据区的最大长度是 65,507 字节 (65,535 - 20 - 8 =65,507)。许多 ping 实现方案允许用户指定大于 65,507 字节的封包大小。过大的 ICMP 封包会引发一系列不利的系统反应，如拒绝服务 (DoS)、系统崩溃、死机以及重新启动。

  当启用 Ping of Death选项时，DPF-Series 设备检测并拒绝这些过大的且不规则的封包大小，即便是攻击者通过故意分段来隐藏总封包大小。

- Prevent Tear drop

  Teardrop 攻击利用了 IP 封包碎片的重组。在 IP 包头中，有一个碎片偏移字段，它表示封包碎片包含的数据相对于原始未分段封包数据的开始位置（或"偏移"）。当一个封包碎片的偏移值与大小之和不同于下一封包碎片时，封包发生重叠，并且服务器尝试重新组合封包时会引起系统崩溃，特别是如果服务器正在运行含有这种漏洞的旧版操作系统时更是如此。

- Binding Mode

  对报文的 MAC、VLAN 或者 PORT 进行绑定检查

- Prevent Fragment Flood Attack

  当分片报文太多，以至于影响设备的性能时，就发生了分片泛滥。当启用分片洪泛攻击功能时，可以设置一个临界值，一旦超过此值就会调用分片洪泛攻击保护功能。如果超过了该临界值，DPF-Series 设备在该秒余下的时间内会忽略其它的分片报文。

- Prevent ICMP Flood Attack

  当 ICMP 回应请求超出了设备的最大限度，以至于受害者耗尽所有资源来进行响应，直至再也无法处理有效的网络信息流时，就发生了 ICMP 泛滥。当启用了 ICMP 洪泛攻击功能时，可以设置一个临界值，一旦超过此值就会调用 ICMP 洪泛攻击保护功能。如果从一个或多个源向单个目标发送的 ICMP 数据报数超过了此临界值，DPF-Series 设备在该秒余下的时间内会忽略其它的 ICMP 回应要求。

- Prevent UDP Flood Attack

  与 ICMP 洪泛相似，当攻击者以减慢受害者速度为目的向该点发送含有 UDP 数据报的 IP 封包，以至于受害者再也无法处理有效的连接时，就发生了 UDP 泛滥。当启用了 UDP 洪泛攻击功能时，可以设置一个临界值，一旦超过此临界值就会调用 UDP 洪泛攻击保护功能。如果从一个或多个源向单个目标发送的 UDP 数据报数超过了此临界值， DPF-Series 设备在该秒余下的时间内会忽略其它到该目标的 UDP 数据报。

- Source MAC Lock

  将 IP 和 MAC 绑定起来，产生一一对应的关系。当启用了**源 MAC 锁定**，如果设备的 IP 改变了，就不允许此封包通过。

- Prevent TCP SYN Flood Attack

  当主机中充满了无法完成的连接请求的 SYN 报文，以至于主机无法再处理合法的连接请求时，就发生了 SYN 泛滥。DPF-Series 设备可以对每秒钟允许通过防火墙的 SYN 报文个数加以限制，当每秒的 SYN 报文的个数超过这些临界值时，就阻止这些 SYN 报文通过。下图是启用 **TCP SYN 洪泛攻击**的配置：

Prevent TCP SYN Flood Attack		◉ Enable ○ Disable	
By Source IP	Threshold: 20	By Dest IP	Threshold: 50
Drop Defence	Threshold: 60	Finger	☐
Send Reset	○ Enable ◉ Disable	Drop First	◉ Enable ○ Disable

下面对相关的参数予以说明：

- ✧ By Source IP： 同一源 IP 的 SYN 报文，后面的 **Threshold** 是指对应的阀值
- ✧ By Dest IP： 同一目的 IP 的 SYN 报文，后面的 **Threshold** 是指对应的阀值
- ✧ Drop Defence：同一目的 IP 的 SYN 报文的丢弃处理，后面的 **Threshold** 是指对应的阀值
  这里针对上图配置的阀值阐述一下报文的丢弃方法：当每秒钟收到同一目的 IP 地址的 SYN 报文超过 50 但小于 60 时，就看这些 SYN 报文中的 同一源 IP 的个数是否超过 20，如果低于 20 就让报文通过，如果高于 20，那么 DPF-Series 设备在后续 10 秒内丢弃以这些地址(数目超过 20 的地址)为源的 TCP SYN 报文；如果每秒钟收到的同一目的 IP 的 SYN 报文超过 60，那么 DPF-Series 设备在后续的 10 秒内丢弃所有的TCP SYN 报文，这时就不看源 IP 地址了。
- ✧ Finger：特征识别，下一接将详细描述
- ✧ Send Reset：如果启用此功能，当报文丢弃时，就发一个 TCP Reset 报文给攻击者
- ✧ Drop First：如果启用此功能，对于所有第一次收到的 TCP SYN 报文都丢弃

20.3 签名控制（SIGNATURE）

DPF-Series 设备内置了对报文内容字段进行深入的检测和控制，用一个库文件将需要阻止的攻击报文中某些字段的内容收集起来。将这个库文件下载到 DPF-Series 设备中，那么当攻击报文的某些字段与库文件里的内容匹配时，此攻击就被过滤。库文件是专门的企业制定的，各个地区的不一样，可以购买或者在网上下载免费的库文件。

20.4 协议异常报文检测

DPF-Series 设备内置了对协议报文进行深入的检测，可以对于异常的协议报文进行控制，从而保护企业内部服务器免受攻击。目前 DPF-Series 设备支持对 SMTP、POP3、SIP 和 FTP 四种协议的检测。

20.5 扫描攻击

当攻击者先知道了目标网络的布局(哪些 IP 地址有活动主机)、可能的入口点(在活动主机上哪些端口号是活动的)后，他们就能更好地计划其攻击。为了获得这些信息，攻击者必须执行侦查。DPF-Series 设备提供了几个选项以防止攻击者的侦查尝试，从而可阻碍其获得有关受保护网络和网络资源的重要信息。

IP 扫描

当同一个源 IP 地址在 1 秒内将 10 个（如果阀值设置为10）TCP SYN、UDP、ICMP 封包发送给不同的主机时，即进行了一次 IP 扫描。此方案的目的是将封包(比如是 ICMP 应答请求)发送给各个主机，以期获得至少一个回复，从而查明目标的地址。DPF-Series 设备在内部记录从某一源地址发往不同地址的 ICMP 封包数目。如果阀值设置为 10，那么某个主机在 1 秒内将 ICMP 信息流发送给 10 个地址，则 DPF-Series 设备将其标记为地址扫描攻击，并在后续的 10 秒钟内拒绝来自该主机的第 11 个及其它更多 ICMP 封包。

端口扫描

当同一个源 IP 地址在 1 秒内将 TCP SYN 或者 UDP 封包发送给位于相同或者不同目标 IP 地址的 10 个（如果阀值设置为10）不同端口时，即进行了一次端口扫描。此方案的目的是扫描可用的服务，希望至少会有一个端口响应，从而识别目标的服务。DPF-Series 设备在内部记录从某一源地址扫描的不同端口的数目。如果阀值设置为 10，那么某个主机在 1 秒内扫描了 10 个端口，则 DPF-Series 设备将其标记为端口扫描攻击，并在后续的 10 秒钟内拒绝来自该源地址的其它封包(不论目标 IP 地

址为何)。

使用方法如下：

1. 扫描选项配置

   进入 **安全(SECURITY)->SECURITY Config**，修改人力资源部门（hr-SECURITY，继续上面的例子）的安全配置参数。展开 **IPS**，启用 **IP Scan** 和 **Port Scan**，配置对应的阀值。

   ✧ **Port Scan** 中，如果同时启用 **UDP** 和 **TCP**，那么阀值是指 TCP 和 UDP 端口的总和

   ✧ 可以只启用 **IP Scan** 或者 **Port Scan**，也可以二者都启用

图200.　　安全配置

2. 引用安全配置

   进入 **安全(SECURITY)->安全策略(Policies)->新增(Create New)**，在策略中引用安全配置

图201.　　引用安全配置

21 内容过滤

21.1 简介

内容过滤针对企业深层应用进行防御，可以实现对内容攻击行为的精确匹配，从而对于夹杂在合法内容中的可疑流量进行防御。

21.2 URL 过滤

关键字匹配

DPF-Series 设备支持 URL 过滤，根据站点的域名，可以阻止或允许访问不同的站点。DPF-Series 设备是根据输入的关键字来进行过滤的。所连接站点的域名包括了设置的关键字就阻止访问。这里的关键字匹配是完全匹配才生效。例如，配置的关键字为 www.sina，那么访问 mail.sina.com.cn 或者 news.sina.com.cn 时，由于不能匹配到关键字 www.sina，所以不会被阻止。而访问 www.sina.com.cn 时，可以匹配到关键字 www.sina，所以可以被阻止。如果配置的关键字为 sina，那么 news.sina.com.cn、mail.sina.com.cn 和 www.sina.com.cn 都能匹配到关键字 sina，所有都可以被阻止。

配置过程如下：

1. 增加过滤列表

   进入 **安全(SECURITY)-> Content Filter ->URL Filter->新增(Create New)**，增加一个 URL 过滤列表(系统默认有一个名为 default-filter的列表)：

新增URL过滤	提交 取消 返回
URL过滤	sina filter

图202. URL过滤

2. 配置过滤的内容

   进入 **安全(SECURITY)-> Content Filter ->URL Filter**，点击“filter sina”后面的“**Detail**”按钮，添加需要过滤的关键字

URL过滤列表 新增

序号	文件类型	操作
共 2 条记录		
1	default-filter	
2	sinafilter	

图203. URL过滤

再点击“**新增(Create New)**”按钮，便可添加需要过滤的域名的关键字列表：

新增URL过滤	提交 取消 返回
URL过滤	sina.com

图204. URL过滤

再点击“**新增(Create New)**”按钮，可添加其它关键字列表。例如，再添加一个“sohu”关键字：

URL过滤列表		新增
序号	文件类型	操作
共 4 条记录		
1	default-filter	
2	sinafilter	
3	sina-com	
4	sohu	

图205.　　URL过滤

3. 安全配置

   进入 **安全(SECURITY)->SECURITY Config**，可以新增安全配置条目，也可以使用默认安全配置条目。默认有 loose 和 strict 两个。缺省情况下，loose 不启用任何安全配置参数，strict 启用默认安全配置参数。下面修改 loose 的安全配置参数，启用“URL Filter”，选刚才配置的“sina filter”

新增安全配置	提交 取消 返回
名称	Loose
▼ IM/P2P	
IM Profile	im_permit_all
P2P Profile	p2p_permit_all
▶ 内容过滤	
▶ IPS	
▶ 协议异常	

图206.　　安全配置

4. 引用安全配置

   进入 **安全(SECURITY)->安全策略(Policies)->新增(Create New)**，在策略中引用安全配置。这使得所访问的域名中包含了“sina.com”和“sohu”字样的网站都被拒绝。

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 ______ 之前 ⦿ 最后		
安全区			
源安全区	l3-in	目的安全区	l3-out
地址/用户/地址簿			
	⦿ 源 地址 ○ 用户 ○ 地址簿	1.2.2.5-1.2.2.150	
	⦿ 目的地址 ○ 用户 ○ 地址簿		
动作	PERMIT	服务	ANY
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☑ 显示高级	
组			
源组		目的组	
定时计划		安全配置	Loose
双向服务质量			
上行服务质量		下行服务质量	
流量统计	☐		
注释			

图207.　　引用安全配置

注意： 如果配置的关键字为“http://news.sina.com.cn”，则配置不生效，必须把前面的“http://”去掉，配置成“news.sina.com.cn”，方可生效。

库文件匹配

为了简化配置，将需要阻止的网站收集起来组成一个库文件。然后将这个库文件下载到 DPF-Series

设备中，那么当访问的网站和库文件里的网站匹配时，此访问就被拒绝。库文件是专门的企业制定的，各个地区的不一样，可以购买或者在网上下载。

如果选择 FTP 方式升级库文件，首先需要在 FTP 服务器上配置好默认网管，启动FTP服务。配置用户名为target，密码也为target，并将库文件放到 FTP 目录下。

使用过程如下：

1. FTP服务器

   进入 **STSTEM->系统升级(Maintenance)->File Update**，选择 FTP 模式，FTP Server 为 11.1.1.1，端口为 21，用户名/密码 target/target。配置页面如下：

文件服务器	提交 取消 测试
服务器地址	⦿ IP地址 ○ 主机名 11.1.1.1
端口号	21
服务器模式	⦿ FTP 模式 ○ TFTP 模式
用户名和密码	用户名：•••••• 密码：••••••

图208.　　文件服务器

2. 升级库文件

   选择 **System Update->Url-Category**，点击 **Update** 按钮开始升级

系统升级	升级 取消
升级方式	○ HTTP ⦿ FTP/TFTP

系统升级	
○	系统文件
○	配置文件
⦿	库文件
○	ad-rules

升级病毒库	提交 取消
每天	
开始时间	14 时 0 分

图209.　　升级库文件

3. 选择需要过滤的内容

   进入 **安全(SECURITY)-> Content Filter ->URL Category**，可以增加 URL 类型条目，也可以使用默认的条目，这里使用默认的，如下：

URL过滤列表　新增

序号	文件类型	操作
共 5 条记录		
1	default-filter	
2	sinafilter	
3	sina-com	
4	sohu	
5	default_category	

图210.　　URL过滤

点击“**Detail**”按钮进入类型过滤配置页面，然后选择需要过滤的 URL 类型。例如，要过滤带

暴力性的网站：

URL过滤 ：default_category		新增 清除
序号	URL类型	操作
共 0 条记录		

图211.　　URL过滤

4. 安全配置
   进入 **安全(SECURITY)->SECURITY Config**，可以新增安全配置条目，也可以使用默认安全配置条目。默认有 loose 和 strict 两个。缺省情况下，loose 不启用任何安全配置参数，strict 启用默认安全配置参数。修改 loose 的安全配置参数，启用 **URL Category**，选择 default-category

新增安全配置	提交 取消 返回
名称	Loose
▼ IM/P2P	
IM Profile	☐ im_permit_all
P2P Profile	☐ p2p_permit_all
▶ 内容过滤	
▶ IPS	
▶ 协议异常	

图212.　　安全配置

5. 引用安全配置
   进入 **安全(SECURITY)->安全策略(Policies)->新增(Create New)**，在策略中引用安全配置

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 之前 ⦿ 最后		
安全区			
源安全区	l3-in	目的安全区	l3-out
地址/用户/地址簿			
	⦿ 源 地址 ○ 用户 ○ 地址簿	1.2.2.5-1.2.2.150	
	⦿ 目的地址 ○ 用户 ○ 地址簿		
动作	PERMIT	服务	ANY
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☑ 显示高级	
组			
源组		目的组	
定时计划		安全配置	Loose
双向服务质量			
上行服务质量		下行服务质量	
流量统计	☐		
注释			

图213.　　引用安全配置

21.3　内容过滤

DPF-Series 设备可以选择性地封锁通过 HTTP 发送的 ActiveX 控件、Java applet、cookie，或者封锁通过 HTTP（或者 FTP、POP3、SMTP、IMAP）来传输的各种类型的文件（包括 .exe、.txt、.doc 或 .zip 等）。这些组件对网络安全造成的危险是: 它们为不可信方提供了一种手段，使其有可能载入然后控制受保护网络中的主机上的应用程序。当安全策略中启用了对一个或多个这些组件的封锁时，DPF-Series 设备将检查每个到达的包头中列出的内容类型，看看其是否指示封包负荷中有任何目标组件。如果有则封锁这些封包。

DPF-Series 设备对这些组件的封锁分为两部分：

- ♦ 脚本过滤

♦ 文件过滤

文件过滤

DPF-Series 设备可以限制传输的文件的类型和方式，以此来限制用户传输文件和增加安全性。如果下载并运行从 Web 上获得的可执行文件 (比如带有 .exe 扩展名的文件)，并不能保证该文件未受感染。即使您信任下载文件的网站，探测该网站下载请求的某人可能已截取了您的请求，并用修改过的包含恶意代码的.exe 文件做出响应。

文件过滤的使用过程如下：

1. 配置文件过滤列表

   进入 **安全(SECURITY)-> Content Filter ->Block List->File Block**，可以增加 block 列表，也可以使用默认的条目。

   点击“**Detail**”按钮，进入添加文件过滤列表的页面，然后再点击“**新增(Create New)**”按钮，添加需要过滤的文件类型。可以增加多种限制传输文件的方式和类型。

2. 安全配置

   进入 **安全(SECURITY)->SECURITY Config**，可以新增安全配置条目，也可以使用默认安全配置条目。默认有 loose 和 strict 两个。缺省情况下，loose 不启用任何安全配置参数，strict 启用默认安全配置参数。修改 loose 的安全配置参数，启用“Block List”，选择 default-block

图214.　安全配置

3. 引用安全配置

   进入 **安全(SECURITY)->安全策略(Policies)->新增(Create New)**，在策略中引用安全配置

图215.　引用安全配置

脚本过滤

- **Cookie**
  用户访问一个站点，可能由于费用、带宽限制等原因，并不希望浏览网页所有的内容。Cookie 可根据个人喜好进行栏目设定，即时、动态地产生用户所要的内容，这就迎合了不同层次用户的访问兴趣，减少用户项目选择的次数，更合理利用网页服务器的传输带宽。
  由于 Cookie 可以保存在用户机上，并在用户再次访问该 Server 时读回这一特性可以帮助实现很多设计功能，如显示用户访问该网页的次数；显示用户上一次的访问时间；甚至是记录用户以前在本页中所做的选择等等，这可免去再去研究复杂的 CGI 编程。
- **ActiveX 控件**
  Microsoft ActiveX 技术为 Web 设计者提供了创建动态和交互式 Web 页面的工具。ActiveX 控件是允许不同的程序彼此相互作用的组件。例如，ActiveX 允许 Web 浏览器打开电子表格或显示来自后端数据库的个人帐目。ActiveX 组件也可以包含其它组件（如 Java applet）或文件（如 .exe 和 .zip 文件)。
  当访问启用了 ActiveX 的网站时，网站提示将 ActiveX 控件下载到计算机中。Microsoft 提供了一条弹出式消息，显示对供下载的 ActiveX 代码进行认证的公司或编程者的名称。如果信任该代码的来源，则可以继续下载这些控件。如果不信任该来源，则可以拒绝它们。如果将 ActiveX 控件下载到计算机中，则该控件将实现其创建者设计的任何功能。如果这是恶意代码，该控件现在可以重新格式化硬盘、删除所有文件、将您所有的个人电子邮件发送给您的老板，等等。
- **Java Applet**
  与 ActiveX 的用途类似，Java applet 也通过允许与其它程序交互来增强网页的功能。将 Java applet 下载到计算机上的 Java Virtual Machine (VM)。在最初的 Java 版本中， VM 不允许 applet 与计算机上的其它资源交互。从Java 1.1 开始，已放宽了一些限制来提供更强的功能。因此，现在 Java applet 可以访问 VM 外部的本地资源。由于攻击者可以编制 Java applet 来在 VM 外部运行，它们会像 ActiveX 控件那样造成同样的安全威胁。

脚本过滤的使用过程如下：

1. 配置脚本过滤列表
   进入 **安全(SECURITY)->Content Filter ->Block List->Script Block**，可以增加 block 列表，也可以使用默认的条目。

2. 安全配置
   进入 **安全(SECURITY)->SECURITY Config**，可以新增安全配置条目，也可以使用默认安全配置条目。默认有 loose 和 strict 两个。缺省情况下，loose 不启用任何安全配置参数，strict 启用默认安全配置参数。这里为人力资源部门新增一个安全配置参数，启用“Block List”，选择 hr

新增安全配置	提交 取消 返回
名称	hr-secuirty
▼ IM/P2P	
IM Profile	☐ im_permit_all
P2P Profile	☐ p2p_permit_all
▶ 内容过滤	
▶ IPS	
▶ 协议异常	

图216.　　安全配置

3. 引用安全配置
   进入 **安全(SECURITY)->安全策略(Policies)->新增(Create New)**，在策略中引用安全配置

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在 [ ] 之前 ⦿ 最后		
安全区			
源安全区	l3-in	目的安全区	l3-out
地址/用户/地址簿			
	⦿ 源 地址 ○ 用户 ○ 地址簿	10.1.1.5-10.1.1.150	
	⦿ 目的地址 ○ 用户 ○ 地址簿		
动作	PERMIT	服务	ANY
日志	☐ log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☑ 显示高级	
组			
源组		目的组	
定时计划		安全配置	
双向服务质量			
上行服务质量		下行服务质量	
流量统计	☐		
注释			

图217. 引用安全配置

注意： 脚本过滤和文件过滤共用一个列表，这个列表叫做内容过滤列表。也就是说，一个内容过滤列表中包含了脚本过滤和文件过滤，可以同时启用脚本过滤和文件过滤，也可以只启用其中一种。在安全配置里就引用这个内容过滤列表。

21.4 URL 免除

有时候并不希望对所有网站进行脚本过滤，当确认 ActiveX、Applet 或 Cookie 包含的内容是安全的，可以利用 URL 免除功能免掉对特定网站进行脚本过滤。ActiveX 的免除方式不同于 Applet 和 Cookie，下面分别说明。

Applet 和 Cookie 免除

继续“**脚本过滤**”一节的例子，为人力资源部门配置了脚本过滤（同时过滤 ActiveX、Applet 和 Cookie）。现在要免除新浪和 163 网站的 Applet 和 Cookie 过滤。使用过程如下：

1. 配置 URL 免除列表

   进入 **安全(SECURITY)-> Content Filter ->URL Exempt**，可以增加 URL 免除列表，也可以使用默认的条目，这里为人力资源部门增加一个 URL 免除列表，如下：

URL免除列表 （新增）

序号	文件类型	操作
共 1 条记录		
1	default-exempt	

图218. URL免除配置

返回到 **URL Exempt** 配置页面可以看到刚才增加的条目，如下：

新增URL免除	提交 取消 返回
URL免除	hr-empty

图219. URL免除配置

点击“hr-exempt”操作栏的“**Detail**”按钮，进入添加 URL 免除列表的页面，然后再点击“**新增(Create New)**”按钮，添加需要免除的网站的关键字。例如，要免除 sina 和 163 网站的脚

本过滤，配置如下：

新增URL	提交 取消 返回
URL	sina

图220.　　URL免除配置

同理添加 163 网站，添加完成后，结果如下：

URL免除 ：hr-empty　　新增　清除

序号	文件类型	操作
共 2 条记录		
1	sina	
2	163	

图221.　　URL免除配置

2. 安全配置

进入 **安全(SECURITY)->SECURITY Config**，修改人力资源部门的安全配置参数，启用“Block List”，选择 hr；同时启用“URL Exempt”，选择 hr-exempt

当前安全配置　　新增

序号	名称	操作
共 4 条记录		
1	Loose	
2	Strict	
3	default-exempty	
4	hr-exempty	

图222.　　安全配置

3. 引用安全配置

进入 **安全(SECURITY)->安全策略(Policies)->新增(Create New)**，在策略中引用安全配置

新增安全策略　　提交　取消　返回

位置	○ 置顶 ○ 在 ____ 之前 ⊙ 最后		
安全区			
源安全区	l3-in	目的安全区	l3-out
地址/用户/地址簿			
	⊙ 源 地址 ○ 用户 ○ 地址簿	10.1.1.5-10.1.1.150	
	⊙ 目的地址 ○ 用户 ○ 地址簿		
动作	PERMIT	服务	ANY
日志	☐ log		
防病毒	☐ 防病毒		
使能	⊙ 启用 ○ 禁用	☑ 显示高级	
组			
源组		目的组	
定时计划		安全配置	hr-security
双向服务质量			
上行服务质量		下行服务质量	
流量统计	☐		
注释			

图223.　　引用安全配置

ActiveX 免除

由于某个网站的 ActiveX 控件并不是放在本网站上，而是放在专门管理 ActiveX 控件的网站。所以免除的时候，不能输入本网站的域名包含的关键字来免除，而是要输入 ActiveX 控件所在网站的域名包含的关键字。

继续“**Applet 和 Cookie 免除**”一节的例子。现在要免除 Flash 控件的过滤。由于 Flash 控件所在网站的域名包含关键字 flash，所以只需要输入 flash 即可。

只需要在 URL 免除列表 hr-exempt 所包含的免除内容里添加一条即可，其它的配置和“**Applet 和 Cookie 免除**”相同。

进入 **安全(SECURITY)-> Content Filter ->URL Exempt**，显示所有的免除列表：

URL免除列表　　新增

序号	文件类型	操作
共 2 条记录		
1	default-exempt	
2	hr-empty	

图224.　　URL免除配置

点击“hr-exempt”操作栏的“**Detail**”按钮，进入添加 URL 免除列表的页面，然后再点击“**新增(Create New)**”按钮，添加需要免除的网站的关键字 flash，如下：

图225.　　URL免除配置

新增URL　　提交　取消　返回

URL	flash

配置完成后，结果如下：

URL免除 ：hr-empty　　新增　清除

序号	文件类型	操作
共 3 条记录		
1	sina	
2	163	
3	flash	

图226.　　URL免除配置

22 LOG

22.1 简介

DPF-Series 设备支持日志和监控统计功能。所有 DPF-Series 设备都允许在内部 (在闪存中) 和外部 (在日志服务器处) 存储日志数据。尽管在内部存储日志信息很方便，但存储器容量有限。当内部存储器空间完全填满时，DPF-Series 设备就开始用最新的日志条目覆盖最早的条目。为了减轻这种数据丢失，可以将日志存储到外部日志服务器或 WebTrends 服务器中。当新事件和新信息流日志条目产生时，DPF-Series 设备发送到外部存储位置。

下表提供记录数据的可能目标位置:

- 控制台**:** 当您通过控制台来排除 DPF-Series 设备的故障时，这是显示所有日志条目的很有用的目标位置。此外，您可以选择在此只出现报警消息 (关键的、警示的、紧急的)，这样，如果在触发报警时您恰好在使用控制台，即可立即提醒您。
- 内部**:** DPF-Series 设备上的内部数据库是存储日志条目的方便位置，但只有有限的空间。
- 电子邮件**:** 将事件和信息流日志发送给远程管理员的一个方便的方法。
- 日志服务器**:** 由于日志服务器的存储容量比 DPF-Series 设备上的内部闪存大得多，因此，通过将数据发送到日志服务器，可以减轻日志条目超过最大内部存储空间时发生的数据丢失
- WebTrends**:** 允许以图形化的格式查看关键的、警示的和紧急的事件。这需要WebTrends服务器的支持。

注意： 日志的操作应该用 logger 帐号(密码：logger*PWD)，root 帐号(密码：root*PWD)只能查看日志，不能操作日志。

22.2 事件日志

DPF-Series 设备提供事件日志，用于监视系统事件，如由 admin 生成的配置更改，以及自行生成的关于操作行为和攻击的消息和报警。DPF-Series 设备将系统事件按以下严重性级别分类:

- **Emergency (** 紧急**):** 关于 SYN (同步) 攻击、Tear Drop 攻击及 Ping of Death 攻击的消息。
- **Alert (** 警示**):** 关于需要立即引起注意的情况(如防火墙攻击和许可密钥到期)的消息。
- **Critical (** 关键**):** 关于可能影响设备功能的情况，如高可用性 (HA) 状态改变的消息。
- **Error (** 错误**):** 关于可能影响设备功能的出错条件 (如防病毒扫描故障或与 SSH 服务器的通信故障) 的消息。
- **Warning (** 警告**):** 关于可能影响设备功能的情况 (如与电子邮件服务器的连接故障或认证故障、超时以及成功) 的消息。
- **Notification (** 通知**):** 正常事件 (包括 admin 发起的配置更改) 的消息。
- **Information (** 信息**):** 提供一般性系统操作信息的消息。
- **Debugging (** 调试**):** 提供详细调试用途信息的消息。事件日志显示每个系统事件的日期、时间、级别及说明。通过 Web 或 CLI 可以查看 DPF-Series 设备的闪存中存储的每一类事件。

查看事件日志

通过使用 CLI 或 Web 可以查看设备中存储的事件日志。可按模块名、严重级别、信息 id、开始/结束时间、包含的关键字、不包含的关键字、网管（包括管理员名、IP 和网管方式）等条件或条件组合来查询(或者过滤)事件日志。不选择任何过滤条件，就是查询所有的日志。查询的结果可以按照时间的升序或者降序来排序。缺省情况下，按照时间降序排列。下面通过 Web 列举几种不同的过滤条件

来查询事件日志的方法和结果。为简单起见，没有列举所有的情况。

1. 按照默认条件来查询

进入**系统监控和日志(LOG&MONITOR)->Syslog->Event Log**，点击‘**query**’按钮。查询结果按照时间降序排列

Syslog Result

Index	Admin	Time	Module	Level	Method	Message ID	Message
Page:1							
1		2006-2-14 15:32:29	ipsec	notification	bootup	12012	Ipsec module was built run OK.
2		2006-2-14 15:32:29	ssh	notification	bootup	10020	ssh module was built run OK.
3		2006-2-14 15:32:29	zone	notification	bootup	5006	zone module was built run OK.
4		2006-2-14 15:32:29	syslog	notification	bootup	1034	syslog module was built run OK.
5	root	2006-2-14 15:32:28	admin	notification	console	9000	Admin root login successfully from 0.0.0.0 by console.
6		2006-2-14 15:31:48	ipsec	notification	bootup	12012	Ipsec module was built run OK.
7		2006-2-14 15:31:48	ssh	notification	bootup	10020	ssh module was built run OK.
8		2006-2-14 15:31:48	zone	notification	bootup	5006	zone module was built run OK.
9		2006-2-14 15:31:48	syslog	notification	bootup	1034	syslog module was built run OK.

图227. 按照默认条件查询

2. 按照时间来查询

进入**系统监控和日志(LOG&MONITOR)->Syslog->Event Log**，在 Starting Time 输入‘2006-2-14 15:31:47’在 Ending Time 输入‘2006-2-14 15:31:48”’，点击’**query**’按钮。结果如下：

Syslog Result

Index	Admin	Time	Module	Level	Method	Message ID	Message
Page:1							
1		2006-2-14 15:31:48	ipsec	notification	bootup	12012	Ipsec module was built run OK.
2		2006-2-14 15:31:48	ssh	notification	bootup	10020	ssh module was built run OK.
3		2006-2-14 15:31:48	zone	notification	bootup	5006	zone module was built run OK.
4		2006-2-14 15:31:48	syslog	notification	bootup	1034	syslog module was built run OK.
5	debugger	2006-2-14 15:31:47	admin	notification	ssh	9000	Admin debugger login successfully from 192.168.0.123 by ssh.

图228. 按照时间查询

3. 按照关键字来查询

进入**系统监控和日志(LOG&MONITOR)->Syslog-> Event Log**，在 Including Keyword 里输入‘run’，查询结果如下：

Syslog Result

Index	Admin	Time	Module	Level	Method	Message ID	Message
Page:1							
1		2006-2-14 15:32:29	ipsec	notification	bootup	12012	Ipsec module was built run OK.
2		2006-2-14 15:32:29	ssh	notification	bootup	10020	ssh module was built run OK.
3		2006-2-14 15:32:29	zone	notification	bootup	5006	zone module was built run OK.
4		2006-2-14 15:32:29	syslog	notification	bootup	1034	syslog module was built run OK.
5		2006-2-14 15:31:48	ipsec	notification	bootup	12012	Ipsec module was built run OK.
6		2006-2-14 15:31:48	ssh	notification	bootup	10020	ssh module was built run OK.
7		2006-2-14 15:31:48	zone	notification	bootup	5006	zone module was built run OK.
8		2006-2-14 15:31:48	syslog	notification	bootup	1034	syslog module was built run OK.

图229. 按照关键字查询

22.3 流量日志

DPF-Series 设备可以监视和记录根据先前配置的策略 PERMIT 或 DENY 的信息流，可以为所配置的每个策略启用 Log 选项。这里记录的是一个 Session 的连接起始过程，而不是对这个过程的每个封包监控。当为 PERMIT 信息流的策略启用 Log 选项时，设备会记录该策略所 PERMIT 的信息流。当为 DENY 信息流的策略启用 Log 选项时，设备会记录试图通过该设备，但因该策略而被丢弃的信息流。

信息流日志记录每个会话的下列要素:

- ♦ 连接开始/结束的日期和时间
- ♦ 源 IP 地址和端口号
- ♦ 目的 IP 地地址和端口号
- ♦ 源区段和目的区段
- ♦ 协议类型
- ♦ 会话的持续时间
- ♦ 会话中使用的服务

启用流量日志

要记录 DPF-Series 设备接收到的所有 Session，必须为所有策略启用 Log 选项。要记录特定信息流，只对适用于该信息流的策略启用 Log 选项。要对策略启用 Log 选项，请执行下列操作（这里启用了 HTTP、FTP 和 POP3 日志）:

新增安全策略			提交 取消 返回
位置	○ 置顶 ○ 在	之前 ⦿ 最后	
安全区			
源安全区	ANY	目的安全区	ANY
地址/用户/地址簿			
	⦿ 源 地址 ○ 用户 ○ 地址簿		
	⦿ 目的地址 ○ 用户 ○ 地址簿		
动作	PERMIT	服务	ANY
日志	☑ log		
	☑ http-log ☑ ftp-log ☑ pop3-log ☐ smtp-log ☐ imap-log		
防病毒	☐ 防病毒		
使能	⦿ 启用 ○ 禁用	☐ 显示高级	

图230. 策略中启用log

启用流量日志的时候，先要选中“log”，即打开日志开关。从上图可以看出，这里只列举了五种协议：http-log、ftp-log、pop3-log、smtp-log 和 imap-log。除这五种协议以外的其它协议(如 ICMP)，如需记录日志，只需要开启日志开关。而列举出来的这五种协议，需要记录日志，需要再选中对应的选项即可。

注意：启用了 smtp-log 和 imap-log 后，还需要配置一条 DPF-Series 设备到邮件服务器的主动路由。对于这两种日志，DPF-Series 设备要把邮件的内容收到本地，组合后再自己发送给邮件服务器，所以这时 DPF-Series 设备需要连接到邮件服务器。

另外：IM 日志设置方法请参照 **IM/P2P** 一章

查看流量日志

通过使用 CLI 或 Web 可以查看设备中存储的流量日志。DPF-Series 设备支持通过过滤条件来查询流量日志，可按照源/目的区段、源/目的 IP、策略、协议类型、用户名/用户组、起始/结束时间、服务类型(URL/FTP/EMAIL)、会话最小/最大持续时间等条件或条件组合来查询流量日志。不选择任何过滤条件，就是查询所有的日志。查询的结果可以按照时间的升序或者降序来排序。缺省情况下，按照时间降序排列。下面通过 Web 列举几种过滤条件来查询流量日志的方法和结果。为简单起见，只列举了其中几种。

1. 按照默认条件来查询

进入**系统监控和日志(LOG&MONITOR)->Syslog->Traffic Log**，点击‘**query**’按钮。查询结果按照时间降序排列。

1	2006-2-15 10:4:16	172.16.161.228	172.16.161.233	17	137	137	NetBIOS-NS	none	l2-in	l2-out	19
2	2006-2-15 10:4:10	172.16.161.233	172.16.161.228	6	1865	139	NetBIOS-SSN	none	l2-out	l2-in	13
3	2006-2-15 10:4:0	172.16.161.233	172.16.161.228	1	8	0	PING	none	l2-out	l2-in	3
4	2006-2-15 10:2:48	172.16.161.228	220.181.26.195	6	4213	110	POP3	none	l2-in	l2-out	14
5	2006-2-15 10:2:47	172.16.161.228	218.16.121.102	6	4211	110	POP3	none	l2-in	l2-out	13
6	2006-2-15 10:2:47	172.16.161.228	220.181.12.114	6	4212	110	POP3	none	l2-in	l2-out	13
7	2006-2-15 10:0:46	172.16.161.25	172.16.161.228	17	137	137	NetBIOS-NS	none	l2-out	l2-in	42
8	2006-2-15 10:0:23	172.16.161.228	172.16.161.25	17	138	138	NetBIOS-DGM	none	l2-in	l2-out	19
9	2006-2-15 10:0:19	172.16.161.25	172.16.161.228	6	1927	139	NetBIOS-SSN	none	l2-out	l2-in	13
10	2006-2-15 10:0:10	172.16.161.25	172.16.161.228	1	8	0	PING	none	l2-out	l2-in	4
11	2006-2-15 9:59:46	172.16.161.228	220.181.26.195	6	4186	110	POP3	none	l2-in	l2-out	18

图231. 按照默认条件查询

2. 按照类型来查询

进入**系统监控和日志(LOG&MONITOR)->Syslog->Traffic Log**，这里选择“URL”

注意：URL、FTP、EMAIL(IMAP、SMTP 和 POP3) 和 IM/P2P 的日志在此处查询

流量日志	查询 取消		
地址	☑		
源 IP	-		
目的 IP	-		
服务	☐		
用户与组	☐		
URL/FTP/EMAIL/IM-P2P	☑		
类型	◉ URL ○ FTP ○ EMAIL ○ IM/P2P		
域		网址	
策略	☐		
源安全区		目的安全区	
连接最小时长(秒)		连接最大时长(秒)	
发送/接收	☐		

图232.　　按照类型查询

查询结果如下：

1	2006-2-15 9:54:51	172.16.161.228	202.165.102.129	13	url:
2	2006-2-15 9:46:4	172.16.161.228	211.154.163.216	23	url: www.hiho.com/convert?
3	2006-2-15 9:45:59	172.16.161.228	207.68.178.16	236	url: rad.msn.com/ADSAdClient31.dll?
4	2006-2-15 9:45:59	172.16.161.228	207.68.178.16	236	url: rad.msn.com/ADSAdClient31.dll?
5	2006-2-15 9:45:59	172.16.161.228	207.68.178.16	228	url: rad.msn.com/ADSAdClient31.dll?
6	2006-2-15 9:45:59	172.16.161.228	207.68.178.16	236	url: rad.msn.com/ADSAdClient31.dll?
7	2006-2-15 9:42:47	172.16.161.228	61.151.249.221	14	url:
8	2006-2-15 9:42:24	172.16.161.228	61.152.242.202	12	url: /main/adfshow?
9	2006-2-15 9:42:15	172.16.161.228	207.46.216.62	15	url: c.msn.com/c.gif?
10	2006-2-15 9:42:11	172.16.161.228	207.68.178.16	8	url: rad.msn.com/ADSAdClient31.dll?
11	2006-2-15 9:35:10	172.16.161.228	211.100.33.125	13	url:

图233.　　按照类型查询结果

22.4　命令日志

DPF-Series 设备可以将管理员对设备进行配置的过程记录下来，以便查询。命令日志记录的内容包括：

- ♦ 管理员登录的用户名和 IP
- ♦ 连接方式(例如，HTTP、Telnet、SSH 等)
- ♦ 登录的时间
- ♦ 执行的命令

查看命令日志

通过使用 CLI 或 Web 可以查看设备中存储的命令日志。DPF-Series 设备支持通过过滤条件来查询各项命令日志的，可按登录的用户名、起始/结束时间包含的关键字、不包含的关键字等条件或条件组合来查询命令日志。不选择任何过滤条件，就是查询所有的日志。查询的结果可以按照时间的升序或者降序来排序。缺省情况下，按照时间降序排列。下面通过 Web 列举使用不同的过滤条件来查询命令日志的方法和结果。为简单起见，只列举了其中几种。

1. 按照默认条件来查询

   进入**系统监控和日志(LOG&MONITOR)->Syslog->Command Log**，点击‘**query**’按钮。查询结果按照时间降序排列。

Command Syslog Result

Index	Admin	IP	Access-Method	Time	Return	Command
Page:1						
1	root	172.16.161.228	http	2006-2-9 17:49:42	0	eum set subscriber static wangbin mac 00-0B-DB-DF-22-7A vid 0 port 255 group priority_group ip 172.16.161.36 hostname
2	logger	172.16.161.23	http	2006-2-9 17:48:16	0	syslog set syslog-server state enable
3	logger	172.16.161.23	http	2006-2-9 17:48:16	0	syslog set syslog-server port 514
4	logger	172.16.161.23	http	2006-2-9 17:48:16	0	syslog set syslog-server host 172.16.161.23
5	root	172.16.161.23	http	2006-2-9 17:46:55	0	logout
6	root	172.16.161.23	http	2006-2-9 17:46:35	0	eum set monitor-port source fe2 dest cpu
7	root	172.16.161.23	http	2006-2-9 17:16:57	0	modify:firewall set policy from ANY to ANY src-addr ANY dst-addr ANY src-group dst-group action permit service ANY schedule log-type none bandwidth status enable

图234. 按照默认条件查询

2. 按照命令包含的关键字来查询

进入 **系统监控和日志(LOG&MONITOR)->Syslog->Command Log**，在 including keyword 里输入：vif，点击‘**query**’按钮，查询结果如下：

搜索结果

序号	管理员	IP	接入方式	时间	返回值	命令
当前第 1 页						
1	root	192.168.0.111	https	2007-04-30 18:04:08	0	new:firewall set policy from ANY to ANY src-addr ANY dst-addr AN src-group dst-group action permit service ANY schedule log-type http-log ftp-log pop3-log bandwidth status enable
2	root	192.168.0.111	https	2007-04-30 17:58:43	0	ad set exempt-url exempt-url-list hr-empty url flash
3	root	192.168.0.111	https	2007-04-30 17:57:10	0	ad set filter-url-list hr-exempt
4	root	192.168.0.111	https	2007-04-30 17:55:30	0	firewall set security-profile profile-name hr-security
5	root	192.168.0.111	https	2007-04-30 17:53:25	0	firewall set security-profile profile-name hr-exempty
6	root	192.168.0.111	https	2007-04-30 17:53:10	0	firewall set security-profile profile-name default-exempty
7	root	192.168.0.111	https	2007-04-30 17:51:44	0	ad set exempt-url exempt-url-list hr-empty url 163
8	root	192.168.0.111	https	2007-04-30 17:51:34	0	ad set exempt-url exempt-url-list hr-empty url sina
9	root	192.168.0.111	https	2007-04-30 17:51:03	0	ad set exempt-url-list hr-empty
10	root	192.168.0.111	https	2007-04-30 17:35:15	0	ad set filter-url-list default_category

图235. 按照关键字查询

22.5 日志存储空间

系统默认为各种日志分配了 8448 KB 字节的空间，当日志写满时就会发生溢出。溢出的方式采用 FIFO 的方式。可以按需修改日志的存储空间，范围在 100～67584 KB 之间。举例配置如下。

进入 **系统监控和日志(LOG&MONITOR)->Log Setting-> Size**，出现 Size 配置主界面：

容量设置

虚拟系统	事件日志(KByte)	命令日志(KByte)	监控日志(KByte)	流量日志(KByte)	上网记录(KByte)	黑名单日志(KByte)	容量总计(KByte)	操作
共 1 条记录								
root_sys	7680	7680	7680	7680	7680	7680	46080	

所有虚系统当前日志容量总计 308 (KByte)

日志状态

虚拟系统	事件日志(KByte)	命令日志(KByte)	监控日志(KByte)	流量日志(KByte)	上网记录(KByte)	黑名单日志(KByte)	当前容量总计(KByt
共 1 条记录							
root_sys	92	96	24	24	24	24	296

图236. 日志容量设置

点击‘**Edit**’按钮修改日志存储空间：

修改容量设置			提交 取消 返回
虚拟系统名称	root_sys		
事件日志(KByte)	9000	命令日志(KByte)	1000
流量日志(KByte)	8000	上网记录（KByte）	6000
黑名单日志（KByte）	9500		

图237.　　修改日志存储容量

22.6　日志报告

DPF-Series 设备可以将达到预定义的严重性级别（参阅**"事件日志"**中的严重性级别列表）的事件日志，以及其它日志（包括：命令日志、流量日志、监控日志、用户在线日志和用户黑名单日志）发送到指定的日志服务器。缺省情况下，DPF-Series 设备通过 UDP（端口 514）将消息发送到日志服务器。DPF-Series 设备也可以将事件日志以 Email 的方式发送给管理员，方便管理员远程管理。

日志服务器

通过使用 CLI 或 Web 可以为设备配置日志服务器，也可以选择哪些日志需要发送到服务器上，哪些需要记录到本地。也可以同时选择记录到本地和发送到服务器上。下面列举 Web 的配置方法。

1. 日志服务器配置

进入 **系统监控和日志(LOG&MONITOR)->Log Setting-> Log Server,** 点中'**Enable**'，配置服务器地址和端口

日志服务器设置	提交 取消
日志服务器设置	⦿ 启用 ○ 禁用
日志服务器地址	172.16.161.23
日志服务器端口	514

图238.　　日志服务器配置

2. 日志过滤配置

进入 **系统监控和日志(LOG&MONITOR)->Log Setting-> Filter**，配置如下：

Log Setting　　Apply　Cancel

Log Type	Internal	Log Server	WebTrends Server
Command Log	☑	☐	☐
Monitor Log	☑	☑	☐
Traffic Log	☐	☑	☐
Online Log	☑	☐	☐
Black-list Log	☑	☑	☐

图239.　　日志过滤配置

3. 事件日志过滤配置

对于事件日志，可以定义日志的严重级别，以下是过滤事件日志的主页面：

Log Filtering						
Module	**Console**	**Internal**	**Email**	**Log Server**	**WebTrends**	**Operation**
Total:18						
syslog	Error	Notification	Error	Information	Information	
system	Error	Notification	Error	Information	Information	
vsys	Error	Notification	Error	Information	Information	
network	Error	Notification	Error	Information	Information	
zone	Error	Notification	Error	Information	Information	
dhcp	Error	Notification	Error	Information	Information	
eum	Error	Notification	Error	Information	Information	
dot1x	Error	Notification	Error	Information	Information	
admin	Error	Notification	Error	Information	Information	
ssh	Error	Notification	Error	Information	Information	
ha	Error	Notification	Error	Information	Information	
ipsec	Error	Notification	Error	Information	Information	
l2tp	Error	Notification	Error	Information	Information	
firewall	Error	Notification	Error	Information	Information	
iptrack	Error	Notification	Error	Information	Information	
ad	Error	Notification	Error	Information	Information	
rstp	Error	Notification	Error	Information	Information	
rip	Error	Notification	Error	Information	Information	
Total:18						
Module	**Console**	**Internal**	**Email**	**Log Server**	**WebTrends**	**Operation**

图240.　　事件日志过滤配置

可以分别定义每种事件日志的严重级别，如果严重级别选择‘Close’就是关闭某个模块发送事件日志到服务器。例如，定义‘system’的发送到日志服务器的严重级别为 Warning。

进入 **系统监控和日志(LOG&MONITOR)->Log Setting-> Filter**，点击‘system’后面的 ’**Edit**’ 按钮，修改严重级别：

Edit Log Filtering		Apply Cancel Back	
Module	system	Console	Error
Internal	Notification	Email	Error
Log Server	Warning	WebTrends Server	Information

图241.　　修改严重级别

WebTrends 服务器

NetIQ 提供了称为 WebTrends Firewall Suite 的产品，可用于根据 DPF-Series 设备生成的日志创建自定义报告。WebTrends 分析日志文件，并且用图形格式显示所需的信息。可以将流量日志和事件日志发送到 WebTrends 服务器。对于事件日志，可以创建所有事件和严重性级别的报告，或者集中报告某个方面的事件。只要启用了 WebTrends 服务器，事件日志就开始发送到服务器上。而流量日志可以选择是否需要发送。(有关 WebTrends 的其它信息，请参阅 WebTrends 产品手册。)下面列举 Web 的配置方法。

1. WebTrends 服务器配置

进入 **系统监控和日志(LOG&MONITOR)->Log Setting->WebTrends**，点击‘Enable’，配置服务器地址和端口

WebTrends服务器设置	提交 取消
WebTrends服务器	◉ 启用 ○ 禁用
WebTrends服务器地址	172.16.163.23
WebTrends服务器端口	514

图242.　　WEBTrends服务器配置

2. 日志过滤配置

进入 **系统监控和日志(LOG&MONITOR)->Log Setting->Filter**，将流量日志配置发送到 WebTrends 服务器上

Log Setting　Apply　Cancel

Log Type	Internal	Log Server	WebTrends Server
Command Log	☑	☐	☐
Monitor Log	☑	☐	☐
Traffic Log	☑	☐	☑
Online Log	☑	☐	☐
Black-list Log	☑	☑	☐

图243. 日志过滤配置

3. 事件日志过滤配置

可以分别定义每种事件日志的严重级别，如果严重级别选择‘Close’就是关闭某个模块发送事件日志到 WebTrends 服务器。例如，定义‘syslog’的发送到 WebTrends 服务器的严重级别为 Error。

进入 **系统监控和日志(LOG&MONITOR)->Log Setting-> Filter**，点击‘syslog’后面的 ’**Edit**’ 按钮，修改严重级别：

Edit Log Filtering　Apply　Cancel　Back

Module	syslog	Console	Error
Internal	Notification	Email	Error
Log Server	Information	WebTrends Server	Error

图244. 修改严重级别

Email 报告

为方便管理员远程管理，可通过配置邮件将事件日志发送到管理员的电子邮箱中，这样对重大问题能够及时发现和解决。并且在提交前可通过测试功能测试邮件服务器是否连通、发送人和接收人邮件设置是否正确，以及需要认证时邮件发送人的地址和密码是否匹配等。如果出现错误配置，测试功能将会给出提示，如密码错误、服务器连接错误等。如果测试通过，也会给出测试通过的提示。

范例

在本例中，如果事件日志达到预先定义的严重级别，则通过电子邮件警示来设置通知管理员。邮件服务器地址为 mail.abcd.net，邮件的发送者为 shan@abcd.net，通知的第一个电子邮件地址为 shan@abcd.net，第二个地址为 lili@abcd.net，第三个地址为 mei@abcd.net。并且需要密码认证。由于需要连接到邮件服务器，所以首先要配置DNS 服务器。

1. DNS 参数设置

进入 **网络配置(NETWORK)->Protocols->DNS**，至少配置一个 DNS 服务器地址：

DNS 服务器 IP　提交　取消

主用DNS服务器	202.96.134.133
备用DNS服务器1	202.64.12.18
备用DNS服务器2	202.68.128.56

图245. DNS配置

2． Email 参数设置

进入 **系统监控和日志(LOG&MONITOR)->Log Setting->Email setting**，点中‘Enable’，配置 Email 参数：

邮件设置	提交 取消 测试		
邮件功能	⦿ 启用 ○ 禁用		
邮件服务器地址	mail.abcd.net		
邮件服务器端口	25		
邮件发送人地址	shan@abcd.net		
邮件接收人地址1	shan@abcd.net		
邮件接收人地址2	lili@abcd.net		
邮件接收人地址3	mei@abcd.net		
邮件接收人地址4			
邮件接收人地址5			
邮件服务器 认证	⦿ 需要 ○ 不需要		
密码	••••••	确认密码	••••••

图246.　　Email 配置

3． 事件日志过滤配置

可以分别定义每种事件日志的严重级别，如果严重级别选择‘Close’就是关闭某个模块发送 Email。例如，定义‘ha’模块发送 Email 的严重级别为 Warning。

进入 **系统监控和日志(LOG&MONITOR)->Log Setting-> Filter**，点击‘ha’后面的 ’**Edit**’ 按钮，修改严重级别：

Edit Log Filtering		Apply Cancel Back	
Module	ha	Console	Error
Internal	Notification	Email	Warning
Log Server	Information	WebTrends Server	Information

图247.　　事件日志过滤配置

22.7　日志导出

DPF-Series 设备可以将各种日志导出，以文件的方式存放于外部主机上，以便对日志进行存储、整理以及分析和统计等。可以用 FTP 或者 TFTP 来导出日志文件。如果利用 FTP 导出，则首先要在 DPF-Series 设备上配置好 FTP 参数；并在主机上启用 FTP 软件。

可以将以下日志导出：

- 事件日志
- 命令日志
- 流量日志
- 监控日志
- 用户在线日志
- 认证用户黑名单日志

范例

在本例中，将‘2006-2-9～2006-2-10’的事件日志用 FTP 的方式导出。导出的日志存放于 IP 地址

为 172.16.161.23 的主机上，并存放在主机的 FTP 目录下的 event 子目录。这就需要在主机的 FTP 目录下创建 event 子目录。

1．文件服务器参数配置

进入 **系统配置管理(SYSTEM)->系统升级(Maintenance)-> File Server**，配置文件服务器参数，这里使用 FTP。

File Server	Apply Cancel Test
Server	⦿ IP Address ○ Host Name 172.16.161.23
Port	21
Server Mode	⦿ FTP Mode ○ TFTP Mode
Username and Password	Username: •••••• Password: ••••••

图248. 文件服务器配置

2．日志导出参数配置

进入 **系统监控和日志(LOG&MONITOR)->Log Setting-> Export Log**，配置日志导出参数，点击"**Apply**"按钮，即可导出日志。

Export Log			Apply Cancel
Log Type	Event Log	Path	event
Starting Time	2006-2-9	Ending Time	2006-2-10

图249. 日志导出参数

22.8 日志自动备份

DPF-Series 设备可以将各种日志以文件的方式自动备份存放于外部主机上，以便对日志进行存储、整理以及分析和统计等。可以定时备份，也可以溢出时才备份。也可以两种备份都启用。对于定时备份，可以选择每天或者每周定时备份。例如，选择每天的 8 点 5 分 5 秒，或者选择每周星期三的 24 点 1 分 2 秒定时备份。溢出备份是在日志空间写满时，系统自动备份。

与日志导出一样，可以用 FTP 或者 TFTP 来导出日志文件。如果利用 FTP 导出，则首先要在 DPF-Series 设备上配置好 FTP 参数；并在主机上启用 FTP 软件。

可以将以下日志自动备份：

- 事件日志
- 命令日志
- 流量日志
- 监控日志
- 用户在线日志
- 认证用户黑名单日志

范例

在本例中，将流量日志和用户在线日志用 FTP 的方式定时备份，同时当日志空间写满时，启用溢出备份。备份的日志存放于 IP 地址为 172.16.161.23 的主机上，并分别存放在主机的 FTP 目录下的 trffic 和 onlielog 子目录。这就需要在主机的 FTP 目录下创建 trffic 和 onlielog 子目录。

1．文件服务器参数配置

进入 **系统配置管理(SYSTEM)->系统升级(Maintenance)->File Server**，配置文件服务器参数，这里使用 FTP。

文件服务器	提交 取消 测试
服务器地址	○ IP地址 ○ 主机名 192.168.0.170
端口号	69
服务器模式	○ FTP 模式 ⦿ TFTP 模式

图250. 文件服务器配置

2. 自动备份参数配置

进入 **系统监控和日志(LOG&MONITOR)->Log Setting->Auto Back**，出现自动备份主页面：

过滤器设置 | 邮件设置 | 日志服务器设置 | WebTrends服务器 | 容量设置 | 日志导出 | 自动备份

自动备份

日志类型	状态	定期	溢出	路径	操作
事件日志	禁用	禁用	禁用		
命令日志	禁用	禁用	禁用		
流量日志	禁用	禁用	禁用		
上网统计	禁用	禁用	禁用		

图251. 日志自动备份主页面

自动备份

日志类型	状态	定期	溢出	路径	操作
事件日志	禁用	禁用	禁用		
命令日志	禁用	禁用	禁用		
流量日志	禁用	禁用	禁用		
上网统计	禁用	禁用	禁用		

单击‘Traffic Log’后面的‘**Edit**’按钮(上图蓝色框指示)，配置自动备份参数：

流量日志自动备份	提交 取消 返回	
状态	⦿ 启用 ○ 禁用	
定期	○ 禁用 ⦿ 每天 ○ 每周	时 7 分 10 秒 00 星期 星期日
溢出	⦿ 启用 ○ 禁用	
路径	traffic	

图252. 流量日志参数

同理配置用户在线日志的自动备份，配置好的结果如下：

Size | Email setting | Log Server | WebTrends | Filter | Export | Auto Backup

Auto Back

Log Type	Status	Termly	Overflow	Backup Path	Operation
Event Log	Disable	Disable	Disable		
Command Log	Disable	Disable	Disable		
Monitor Log	Disable	Disable	Disable		
Traffic Log	Enable	8:10:20,Everyday	Enable	trffic	
Online Log	Enable	22:1:5,Sunday	Enable	onlinelog	

图253. 在线日志自动备份配置

22.9 日志清除

DPF-Series 设备允许手动删除日志。可以删除命令日志、事件日志、监控日志、流量日志、用户在线日志、认证用户黑名单日志。下面以删除事件日志为例：

进入 **系统监控和日志(LOG&MONITOR)->Syslog ->Clear**，选择要删除的日志类型，输入要删除的日志的时间，单击‘**clear all**’

命令日志 | 事件日志 | 流量日志 | 清除日志

清除日志 清空 取消

日志类别	事件日志
清除此日期以前的日志	NaN-NaN-NaN

图254. 日志清除配置